УТВЕРЖДЕН
RU.48957919.501410-01 И4-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Dallas Lock 8.0

(версия 8.0.761.1)

Инструкция по использованию Сервера конфигураций

RU.48957919.501410-01 И4

Листов 34

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ О СЕРВЕРЕ КОНФИГУРАЦИЙ

1.1 Общие сведения и назначение

Модуль «Сервер конфигураций Dallas Lock» (Сервер конфигураций, СК) — программное средство, предназначенное для контроля за изменением состава программного обеспечения и контроля целостности файлов программного обеспечения (ПО), установленного на компьютерах и серверах в локальной вычислительной сети, составления Проектов паспортов программного обеспечения (Проект паспорта ПО) и утверждения Паспортов программного обеспечения (Паспорт ПО). Паспорт ПО представляет собой заверенную информацию о состоянии программной среды.

Сервер конфигураций позволяет:

- выполнять сбор по сети информации о ПО персонального компьютера (ПК) с установленным СЗИ НСД Dallas Lock 8.0 (СЗИ НСД, DL);
- отслеживать изменения в установленном ПО на клиентах;
- выполнять контроль и фиксацию эталонного состояния СПС;
- формировать Проект паспорта ПО, Паспорт ПО;
- утверждать Паспорт ПО с помощью установки простой электронной подписи (ПЭП);
- создавать и редактировать права учетных записей СК.

В состав программного продукта входят следующие компоненты:

- серверная часть, осуществляющая взаимодействие с клиентскими компонентами, сбор и обработку данных о СПС, контролируемых ПК, хранение данных в базе данных (БД) программного модуля, регистрацию событий;
- Консоль СК, представляющая собой пользовательский интерфейс для управления функциональными возможностями СК, которую можно установить на отдельный ПК;
- клиентская часть, входящая в состав СЗИ НСД.

Сервер конфигураций выполнен в виде отдельного приложения и актуален для средних и больших развертываний СЗИ НСД.

При создании Проекта паспорта ПО в СК производится сканирование файлов контролируемых каталогов с целью вычисления хэш-суммы по алгоритму ГОСТ Р 34.11-2012, а также сохраняются сведения о расположении файлов и метаданные.

1.2 Системные требования

Сервер конфигураций выполнен в виде отдельного программного продукта и предназначен для использования на технических средствах (ТС), таких как ПК, портативные и мобильные компьютеры (ноутбуки и планшетные ПК), серверы.

Минимальная и оптимальная конфигурация ТС определяется требованиями операционной системы. Для установки Консоли СК потребуется не менее 6,6 МБ пространства на системном разделе жесткого диска. Для полной установки компонентов СК потребуется не менее 7,3 МБ пространства на системном разделе жесткого диска.

СК предназначен для работы на ТС, работающих под управлением следующих ОС:

- Windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);
- Windows Server 2008 R2 (SP 1) (Foundation, Standard, Web, Enterprise, Datacenter);
- Windows 8 (Core, Pro, Enterprise);
- Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
- Windows 8.1 (Core, Pro, Enterprise);
- Windows Server 2012 R2 (Foundation, Essentials, Standard, Datacenter);
- Windows 10 (Enterprise, Education, Pro, Home);
- Windows Server 2016 (Multipoint Premium Server, Essentials, Standard, Datacenter, Storage Server, Hyper-V Server);
- Windows Server 2019 (Standard, Datacenter, Essentials)
- Windows 11 (Enterprise, Education, Pro, Home);
- Windows Server 2022 (Standard, Datacenter).

2 УСТАНОВКА И УДАЛЕНИЕ СЕРВЕРА КОНФИГУРАЦИЙ

2.1 Установка Сервера конфигураций

Для установки СК необходимо, чтобы текущий пользователь был локальным администратором ОС Windows, то есть выполнял роль администратора информационной безопасности (администратор ИБ).

Перед установкой СК необходимо включить Windows Firewall (Брандмауэр Windows) для корректного автоматического добавления исключения на TCP-порт 28465. В случае, если установлены иные межсетевые экраны (МЭ), администратор ИБ должен добавить такое исключение для МЭ вручную.

Чтобы установить Сервер конфигураций, необходимо запустить установочный файл DL80.ConfServerSetup.exe и после вывода на экран окна приглашения к установке (Рис. 1) следовать инструкциям установщика:

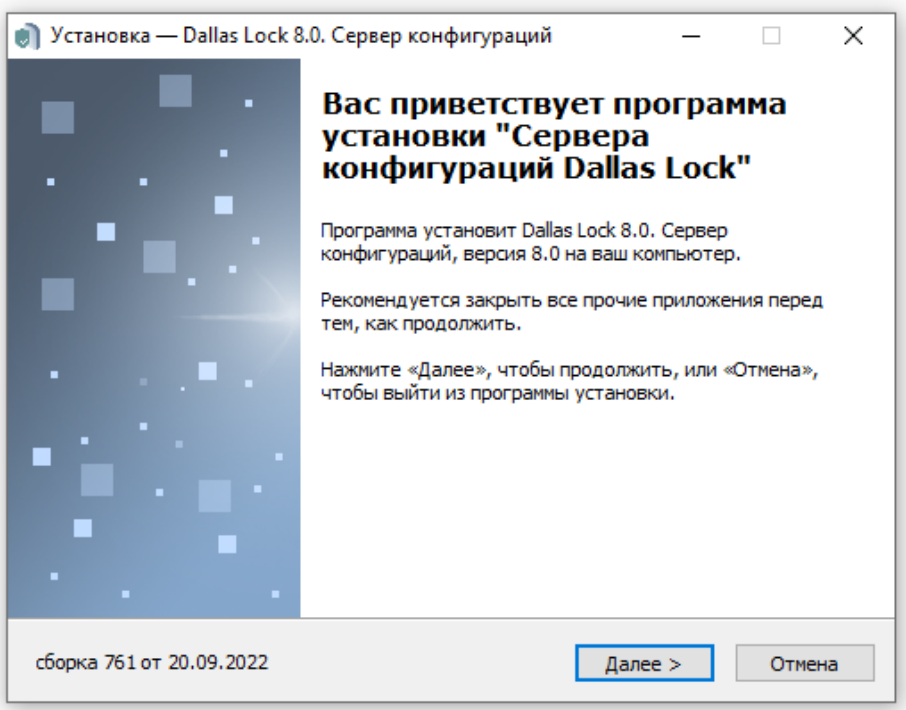


Рис. 1. Окно приглашения к установке

1. Указать номер лицензии и код активации технической поддержки (Рис. 2).

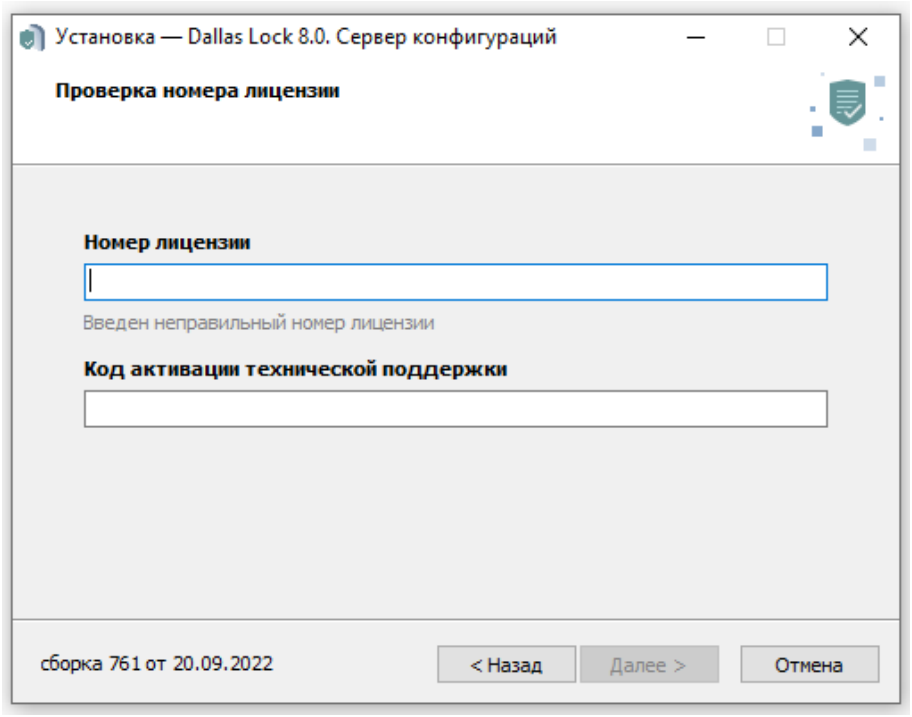


Рис. 2. Окно проверки номера лицензии

2. Выбрать папку для установки либо подтвердить указанную по умолчанию (Рис. 3).

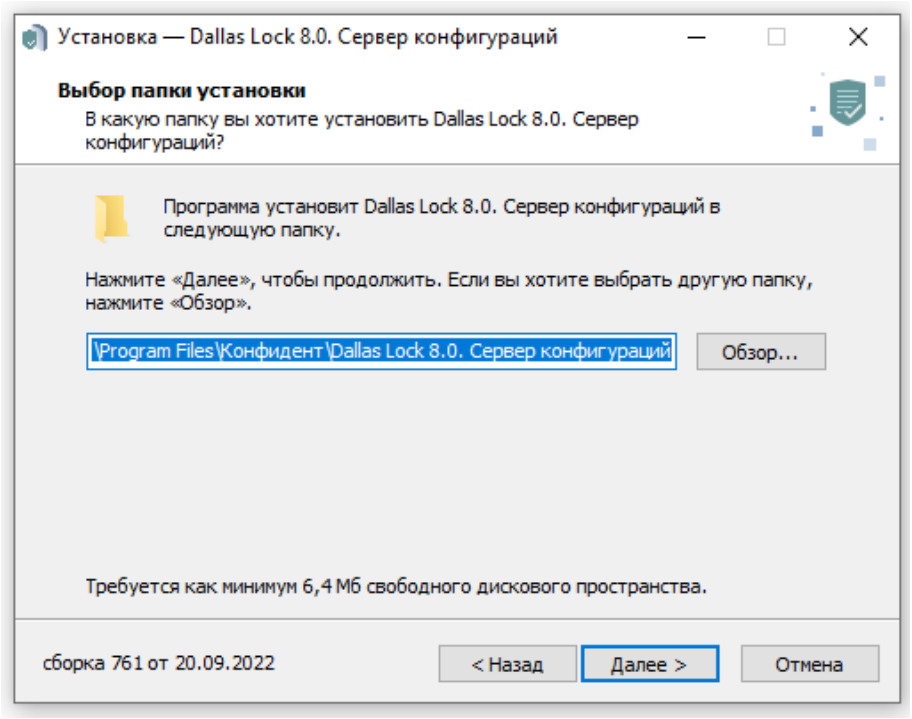


Рис. 3. Окно выбора папки установки

3. Выбрать тип установки (полная (Рис. 4) либо компактная либо выборочная) и компоненты, которые необходимо установить. При этом Консоль СК устанавливается по умолчанию при любом типе установки.

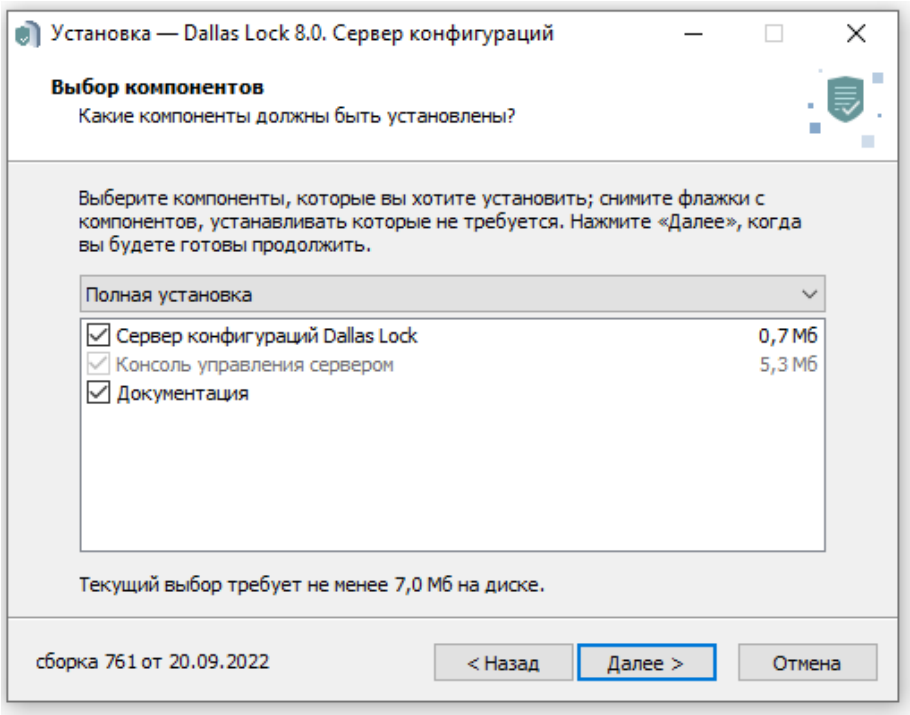


Рис. 4. Окно выбора компонентов

4. Создать аккаунт администратора ИБ (Рис. 5).

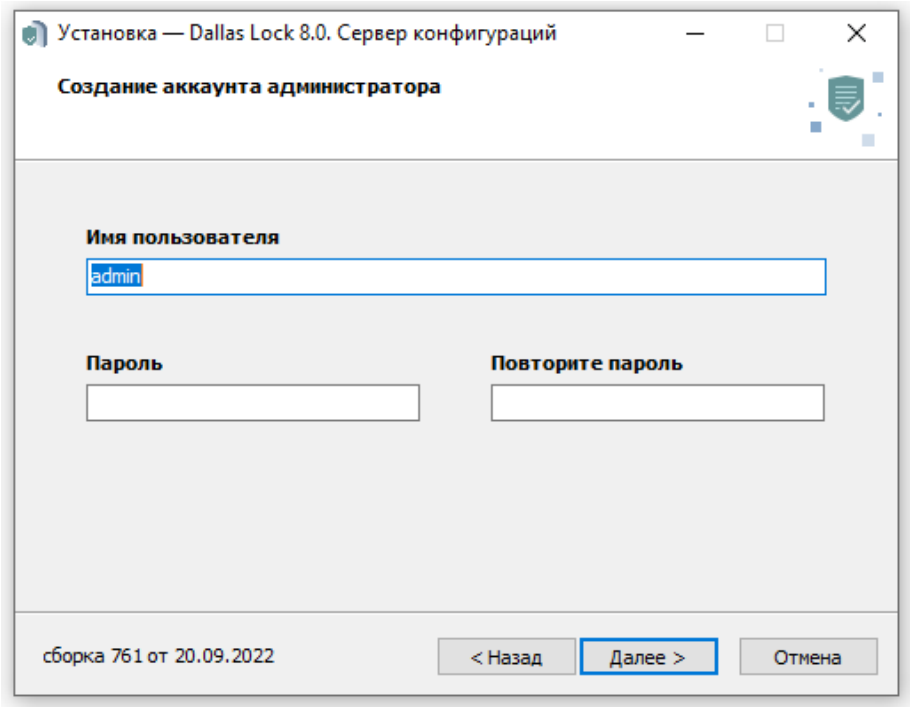


Рис. 5. Окно создания аккаунта администратора ИБ

5. При необходимости выбрать выполнение дополнительных задач (Рис. 6).

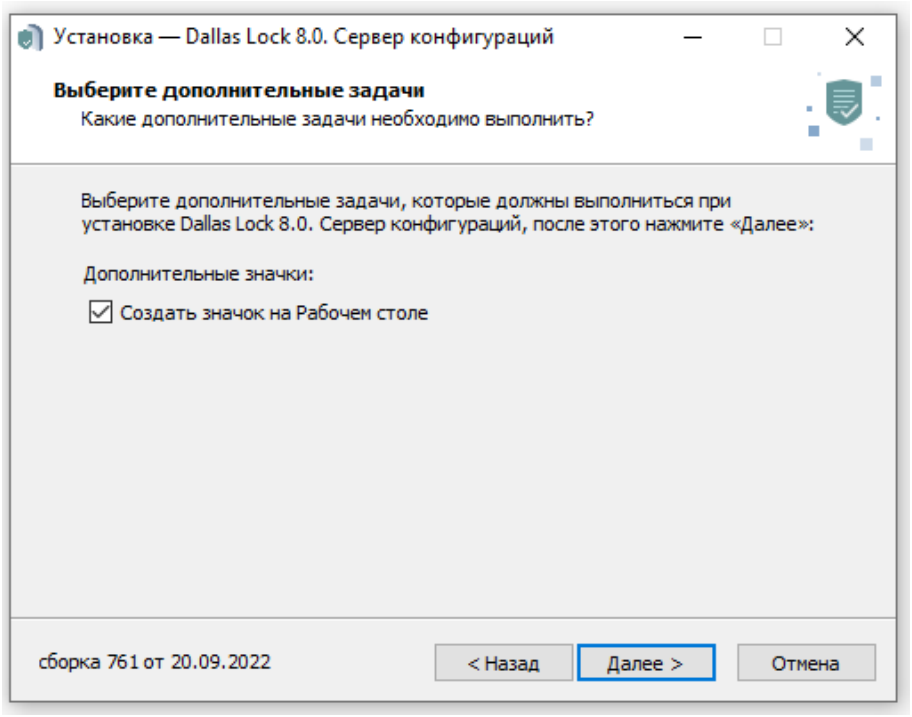


Рис. 6. Окно выбора дополнительных задач

6. Подтвердить все указанные опции установки и нажать кнопку «Установить» (Рис. 7).

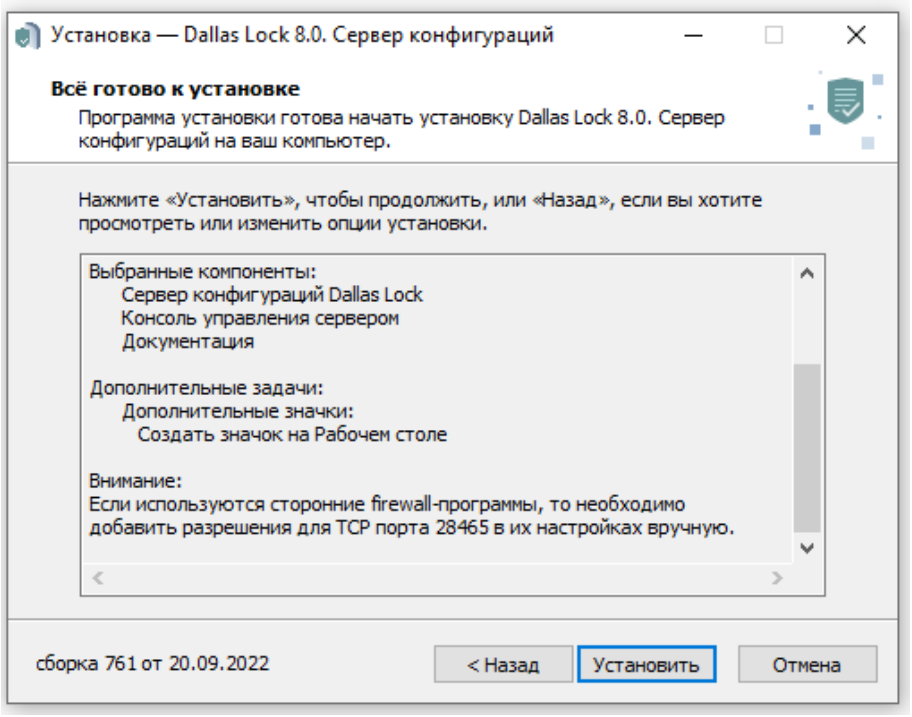


Рис. 7. Окно подтверждения параметров установки

7. Дождаться завершения установки. Успешная установка завершится соответствующим сообщением (Рис. 8).

Рис. 8. Окно успешного завершения установки

После установки СК готов к работе, перезагрузка компьютера не требуется. Установщик Сервера конфигураций создает в меню «Пуск» (и на Рабочем столе, если это было указано при установке) ярлык для запуска Консоли СК.

Примечание. Если СК устанавливается совместно с Сервером безопасности (СБ) или СБ уже установлен, то после установки СК необходимо в Консоли управления СБ в категории «Параметры безопасности домена» во вкладке «Вход», выбрав параметр «Сервер конфигураций», указать параметры подключения к СК: имя сервера, логин и пароль учетной записи администратора ИБ, которая создавалась при установке СК (Рис. 5). Данная возможность доступна только при наличии лицензии на СК.

Если СК устанавливается без СБ, то после установки СК необходимо в Оболочке администратора СЗИ НСД (ОА), перейти в категорию «Параметры безопасности» и во вкладке «Вход», выбрав параметр «Сервер конфигураций», указать вышеперечисленные параметры подключения к СК.

При указании корректных параметров подключения запускается синхронизация политик безопасности с клиентами домена безопасности (ДБ), в БД СК добавляются файлы БД СБ. Используемые данные: список учетных записей ДБ[1], список клиентов.

Выполняется отслеживание добавления и удаления клиентов на СБ: при добавлении либо удалении клиента в БД СБ данный клиент автоматически добавляется в БД СК, либо удаляется из БД СК.

Если СБ не установлен и/или не синхронизован с СК, то в процессе установки в БД СК создаются собственные файлы данных для доменных учетных записей пользователей и клиентов. В процессе дальнейшей эксплуатации СК дублирует эти данные (создание учетных записей) в СБ.

2.2 Удаление Сервера конфигураций

В разных ОС удаление программ может осуществляться по-разному.

В ОС Windows 10 необходимо нажать кнопку «Пуск», выбрать пункт «Параметры», в открывшемся окне выбрать раздел «Приложения». В появившемся окне «Приложения и возможности» из списка выбрать программу «Dallas Lock 8.0. Сервер конфигураций», выбрать действие «Удалить» и подтвердить удаление (Рис. 9). После удаления СК перезагрузка компьютера не требуется.

[1] Используются только учетные записи ДБ, учетные записи AD не «вычитываются».

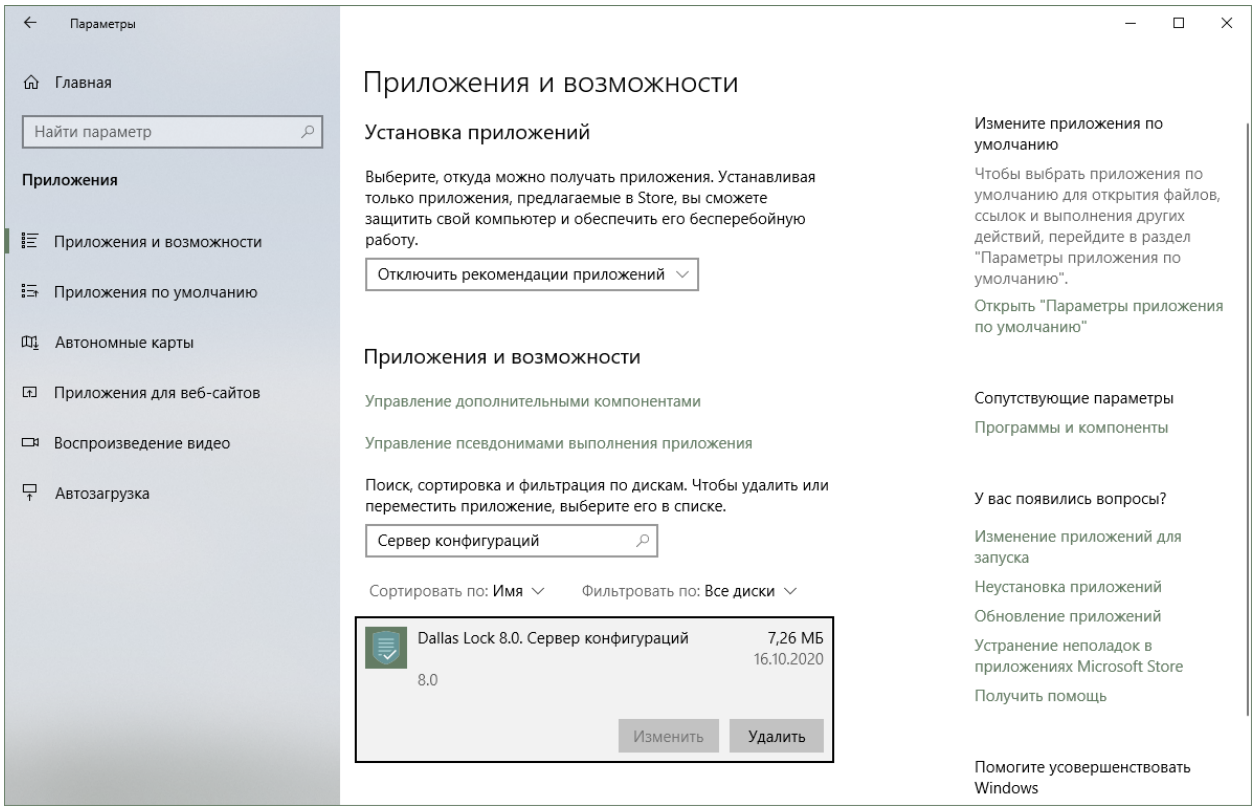


Рис. 9. Удаление СК

3 РАБОТА СЕРВЕРА КОНФИГУРАЦИЙ

3.1 Основы работы

Модуль «Сервер конфигураций Dallas Lock» предназначен для централизованного управления процессами контроля за изменением состава ПО и контроля целостности файлов ПО, установленного на клиентских ПК, составления и утверждения Паспортов ПО.

Основные функциональные возможности Сервера конфигураций:

- сбор и обработка данных о состоянии ПО клиентов;
- формирование Проектов паспорта ПО;
- утверждение Паспортов ПО;
- выполнение сравнений между Проектом паспорта ПО и Паспортом ПО, между Паспортами ПО в рамках одного клиента;
- хранение данных о состоянии ПО клиентов в БД программного модуля;
- регистрация событий;
- централизованная настройка параметров сканирования для контролируемых ПК;
- отслеживание изменений в установленном ПО на клиентах;
- функция сбора по сети и обработки информации о ПО ПК с установленным СЗИ НСД;
- контроль и фиксация СПС.

Сервер конфигураций обеспечивает хранение следующих данных:

- сведения о клиентах;
- сведения о персонале комплекса;
- Паспорта ПО клиентов с электронной подписью Контролеров (информация об изменениях состава ПО и исполняемых файлах);
- информация о ПО;
- состояние ПО клиентов в БД программного модуля.

Управление СК осуществляется с помощью Консоли СК, которая представляет собой пользовательский интерфейс для отображения на экране информации о работе СК.

При запуске Консоли СК необходимо для подключения ввести логин и пароль учетной записи администратора ИБ, созданной при установке СК, а также имя сервера и нажать кнопку «Подключиться» (Рис. 10). Нажатие кнопки «Выход» закроет окно.

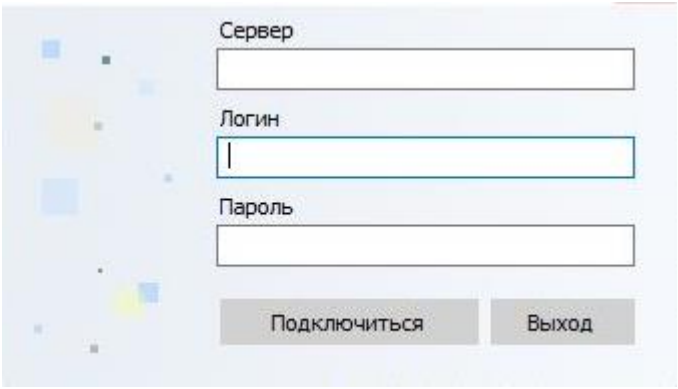


Рис. 10. Окно подключения к СК

При введении неправильного логина и/или пароля администратора ИБ появится сообщение об ошибке подключения по причине неправильного логина или пароля, а также сообщение о неудачном подключении к СК (Рис. 11).

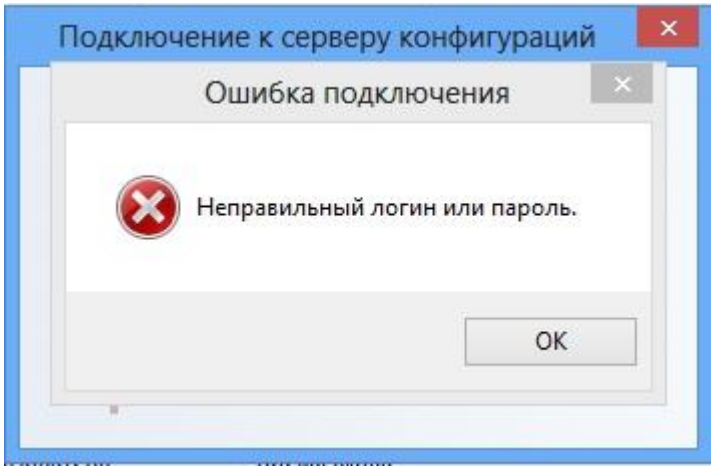


Рис. 11. Ошибка подключения к СК

При введении корректных данных откроется окно Консоли СК. Главное окно Консоли СК содержит следующие рабочие области (Рис. 12):

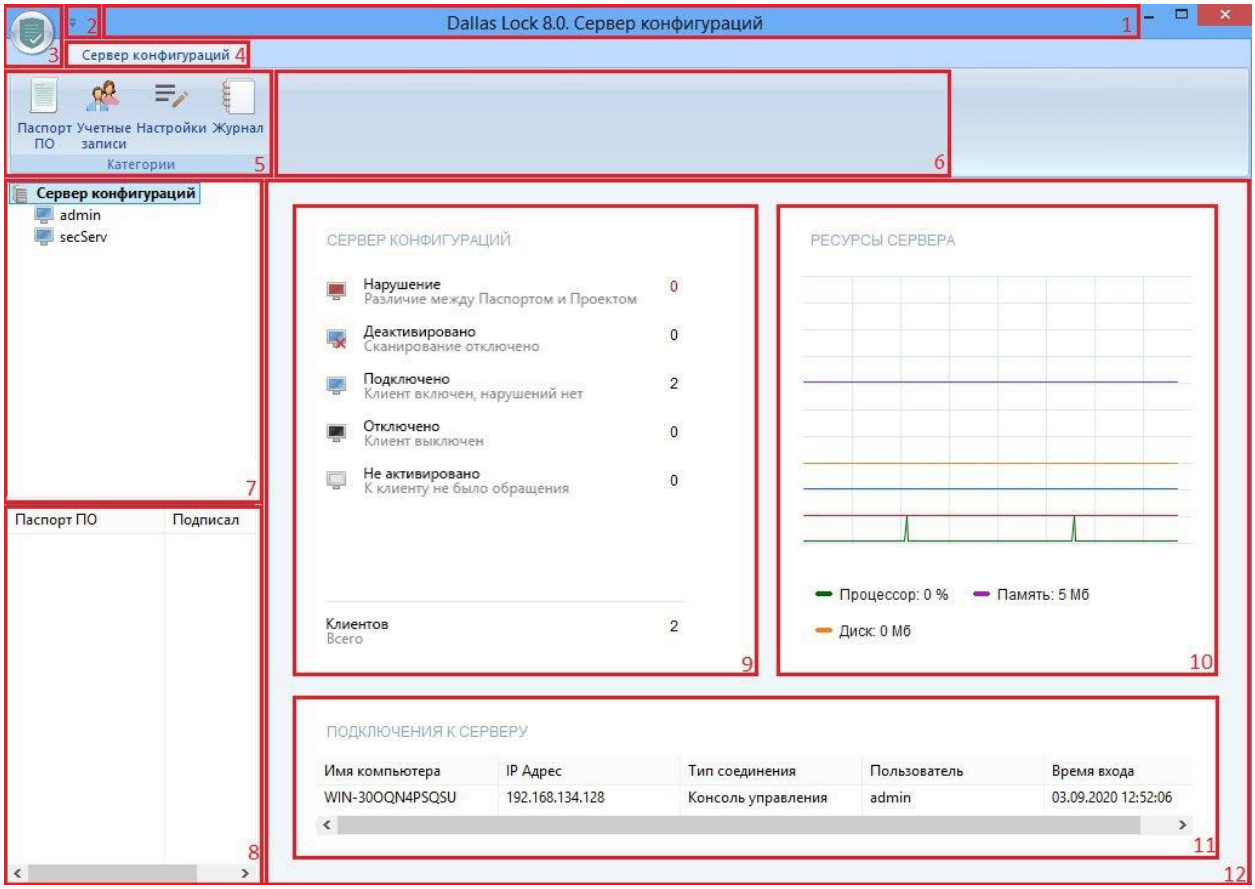


Рис. 12. Вид Сервера конфигураций

1. Заголовок окна (верхняя строка), содержащий название модуля СК.
2. Панель быстрого доступа и ее настройка.
3. Основное меню Консоли СК.
4. Открытая вкладка СК.
5. Лента инструментов со списком основных категорий («Паспорт ПО», «Учетные записи», «Настройки», «Журнал»).
6. Панель инструментов выбранной категории.
7. Дерево объектов СК.
8. Проекты паспорта ПО и Паспорта ПО выбранного клиента.
9. Информация о клиентах СК.

10.График ресурсов СК.

11.Активные подключения к СК.

12.Рабочая область СК.

Нажатие кнопки «Основное меню» в верхнем левом углу с изображением обозначения СК  открывает меню с командами «О программе» и «Выход» (Рис. 13).

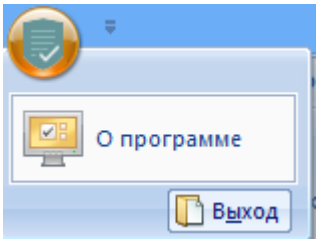


Рис. 13. Вид кнопки «О программе»

Нажатие кнопки «О программе» открывает окно, содержащее следующие сведения о программном продукте (Рис. 14):

- наименование — «Dallas Lock 8.0 Сервер конфигураций»;
- номер и дата выпуска используемой версии продукта;
- указание производителя — «ООО «Конфидент»;
- год выпуска;
- номер лицензии;
- код технической поддержки (при его отсутствии выводится сообщение «Код технической поддержки не задан»).

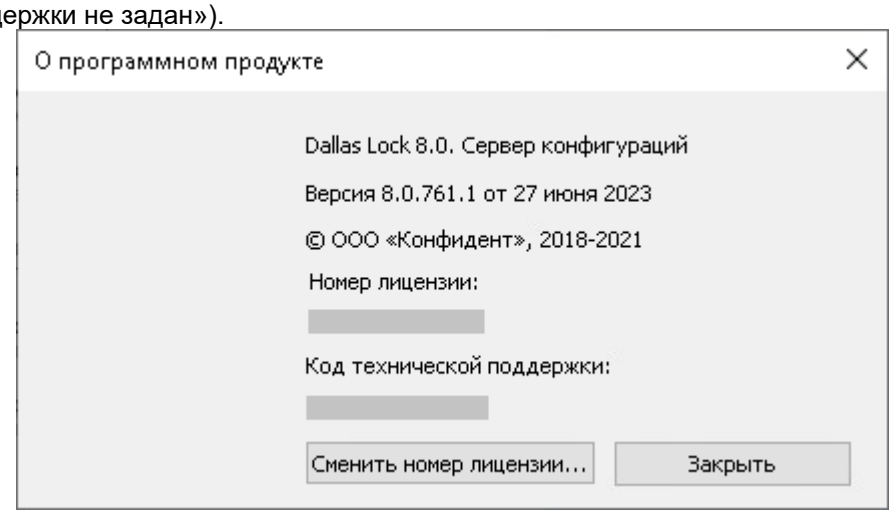


Рис. 14. Информация о программном продукте

В окне сведений о программном продукте для смены номера лицензии продукта используется кнопка «Сменить номер лицензии». Нажатие кнопки «Закрыть» закроет окно.

Для настройки панели быстрого доступа используется кнопка  . При нажатии в контекстном меню выводятся следующие возможности (Рис. 15):

- «Свернуть ленту» — скрывает ленту инструментов со списком основных категорий, при повторном нажатии восстанавливает видимость ленты.
- «Отображать под лентой» — перемещение  в положение под лентой инструментов, команда «Отображать над лентой» возвращает исходное положение.
- «Другие команды». Дает возможность установить (либо впоследствии исключить) на панели быстрого доступа команды, сформировать сочетания клавиш для вызова команд (Рис. 16).

Рис. 15. Настройка панели быстрого доступа

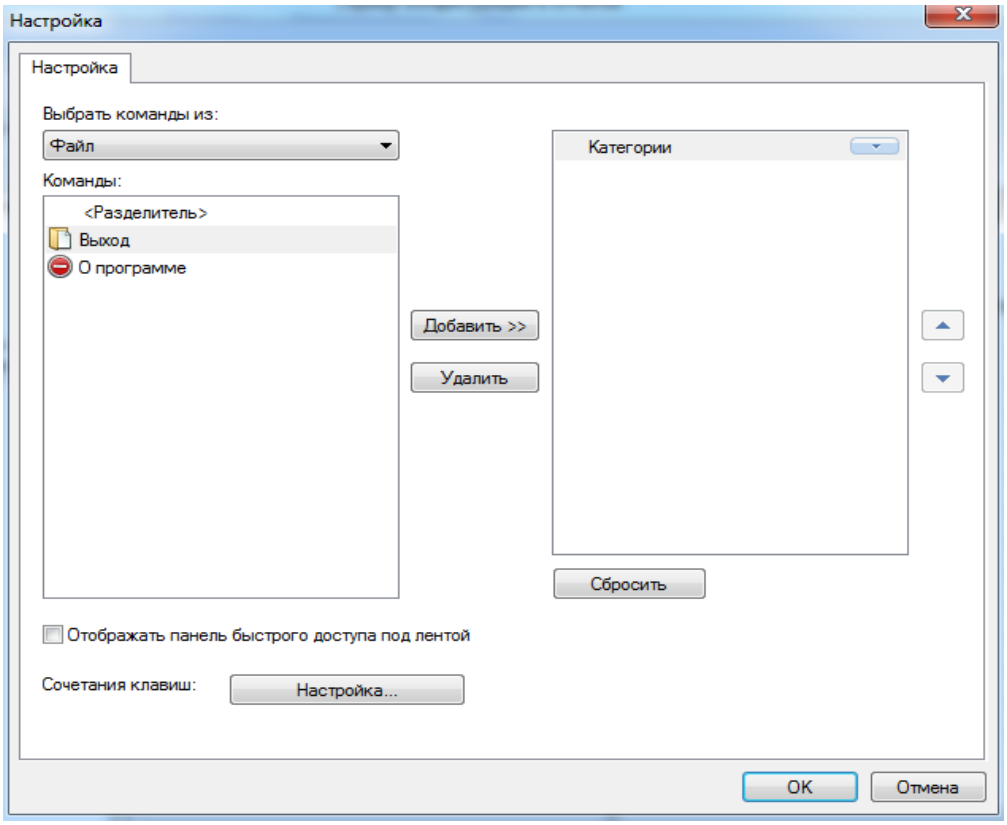


Рис. 16. Настройка других команд

3.2 Использование дерева объектов и рабочей области

В нижней части рабочей области приводится список подключений к серверу, содержащий (Рис. 17):

- имя компьютера,
- IP Адрес,
- тип соединения,
- имя пользователя,
- время входа.

ПОДКЛЮЧЕНИЯ К СЕРВЕРУ

Имя компьютера	IP Адрес	Тип соединения	Пользователь	Время входа
WIN-30OQN4PSQSU	192.168.134.128	Консоль управления	admin	03.09.2020 12:52:06

Рис. 17. Список подключения к серверу

В правой части рабочей области приведен график ресурсов сервера, отражающий (Рис. 18):

- загруженность процессора (%),
- используемый объем память (Мб),
- используемый объем диска (Мб),
- число подключений,
- число операций I/O.

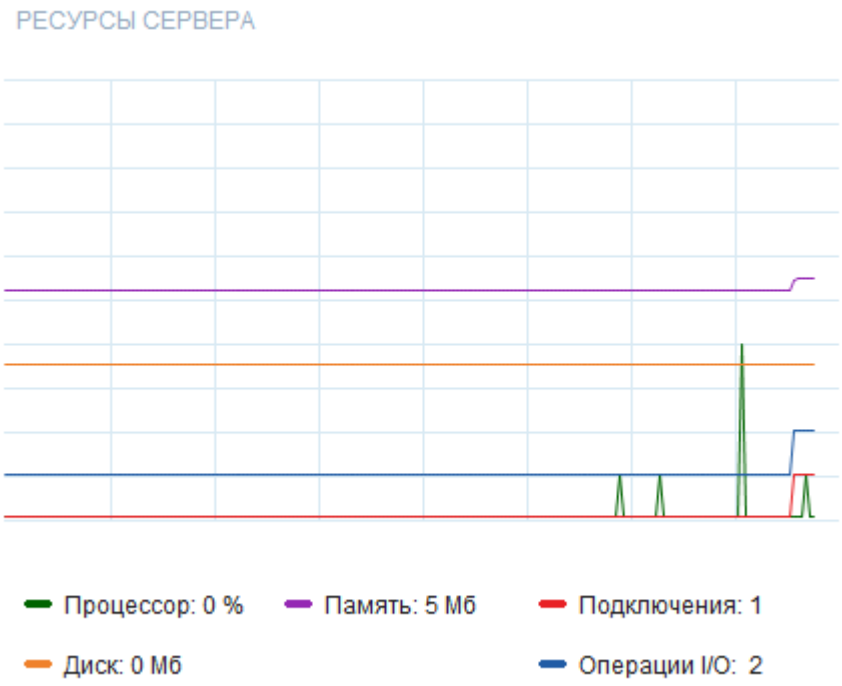


Рис. 18. График ресурсов сервера

Если используется БД СБ DL, то дерево объектов формируется в соответствии с клиентами СБ DL, для всех клиентов устанавливается статус «Не активировано». При обращении клиента к серверу статус обновляется на «Подключено». Если БД СБ DL не используется, то список клиентских машин формируется в момент первого обращения клиента к серверу.

Все новые клиенты первоначально попадают под управление родительского объекта «Сервер конфигураций», пользователь самостоятельно перераспределяет клиентов по группам.

Дерево объектов Консоли СК включает:

- корень дерева «Сервер конфигураций»,
- группы клиентов,
- подгруппы клиентов,
- клиентов.

Клиенты могут находиться в следующих состояниях:

 — нарушение: Проект паспорта ПО отличается от Паспорта ПО;

 — деактивировано: сканирование отключено;

 — подключено: клиент включен, нарушений нет;

 — отключено: клиент выключен;

 — не активировано: к клиенту не было обращения;

 — сканирование: на клиенте проводится сканирование.

В контекстном меню объектов дерева СК для активного узла «Сервер конфигураций» при нажатии правой кнопки мыши выводится список доступных команд (Рис. 19):

- «Добавить клиента» — добавление в дерево объектов автономных клиентов;
- «Добавить группу»;
- «Подписать» — утверждение Проектов паспортов ПО для всех клиентов группы;
- «Выполнить сканирование» — запуск сканирования всех клиентов ДБ.

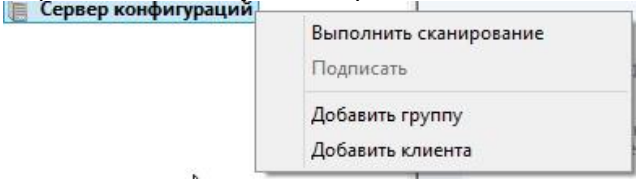


Рис. 19. Доступные команды для активного узла «Сервер конфигураций»

В контекстном меню объектов дерева для активного узла с наименованием группы при нажатии

правой кнопки мыши выводится список доступных команд (Рис. 20):

- «Выполнить сканирование» — запуск сканирования всех клиентов группы.
- «Подписать» — утверждение Проектов паспортов ПО для всех клиентов группы.
- «Добавить подгруппу».
- «Добавить клиента» — добавление в дерево объектов автономных клиентов.
- «Переместить». Администратор ИБ может переместить любую группу в качестве подгруппы в другую группу с помощью команды контекстного меню «Переместить» или перетаскивания значка объекта в поле другого значка. При выборе команды «Переместить» необходимо указать наименование группы, в которую перемещается объект.
- «Переименовать группу». При вызове команды открывается диалоговое окно, в котором необходимо указать новое наименование группы.
- «Удалить группу». Предназначена для удаления группы или подгруппы клиентов, удаление группы или подгруппы с клиентами не реализуется.

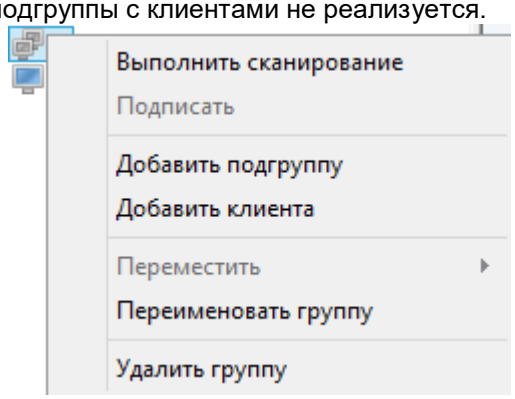


Рис. 20. Доступные команды для активного узла с наименованием группы

В контекстном меню объектов дерева для активного узла с наименованием клиента доступны команды (Рис. 21):

- «Выполнить сканирование» — запуск сканирования выбранного клиента.
- «Подписать» — утверждение Проекта паспорта ПО клиента.
- «Включить сканирование» либо «Отключить сканирование» — подключение модуля «Паспорт ПО» на выбранном клиенте, либо отключение функциональной возможности выполнения сканирования по заданному расписанию/периодичности на клиентском ПК.
- «Переместить». Администратор ИБ может переместить клиента в любую группу с помощью команды контекстного меню «Переместить» или перетаскивания значка объекта в поле другого значка. При выборе команды «Переместить» необходимо указать наименование группы, в которую перемещается объект.
- «Удалить клиента». При удалении клиента, зарегистрированного в БД СК посредством синхронизации с БД СБ, выводится следующее предупреждение: «Внимание! Некоторые из удаляемых клиентов были добавлены посредством СБ. После принудительного удаления таких клиентов на СК следует убедиться, что на СБ политика входа «Сервер конфигураций» для данных клиентов будет в значении «Не задан» (см. политики СБ). Выполнить операцию удаления?» Удаление выполняется только в БД СК, в БД СБ для данного клиента необходимо изменить значение политики «Сервер конфигураций» на значение «Не задан». Если в дальнейшем значение политики «Сервер конфигураций» для такого клиента в БД СБ будет изменено на параметры подключения к СК, то такой клиент будет добавлен в БД СК.

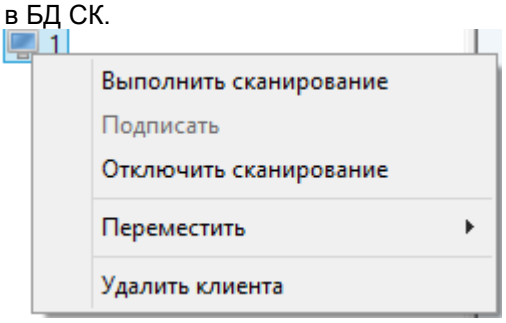


Рис. 21. Доступные команды для активного узла с наименованием клиента

3.3 Группы учетных записей

Предусмотрены следующие группы пользователей:

- аудитор, обладающий полномочиями на просмотр заверенных Проектов паспортов ПО, Паспортов ПО, информации об изменениях в СПС;
- контролер, обладающий полномочиями аудитора, а также полномочиями на заверение Проекта паспорта ПО, на запуск внеочередного сканирования ПК, на загрузку результатов сканирования автономного ПК;
- администратор СК, обладающий полномочиями контролера, а также полномочиями на назначение ролей «Контролер» и «Аудитор», формирование описаний, контролируемых ПК и их групп, управление данными Паспортов ПО, определение параметров работы СК;
- администратор ИБ, обладающий всеми полномочиями администратора СК, а также полномочиями на назначение ролей «Администратор СК» и имеющий возможность настройки конфигурации на автономных ПК.

При установке СК создаётся аккаунт администратора ИБ. После установки СК необходимо авторизоваться в Консоли СК под этой учетной записью пользователя.

Раздел привилегий «Администрирование» включает в себя:

- формирование списка контролируемых ПК;
- формирование групп ПК;
- выполнение операций над клиентами (отключить, включить модуль «Паспорт ПО»);
- просмотр журнала;
- настройка детальности регистрируемых событий (фильтр).

Раздел привилегий «Работа с учетными записями, группами, ролями» включает в себя:

- настройка детальности регистрируемых событий (фильтр);
- управление учетными записями и группами учетных записей (создание и удаление учетных записей и групп, редактирование параметров учетных записей);
- создание учетных записей и групп учетных записей на автономных клиентах и назначение им ролей.

Раздел привилегий «Настройка параметров» включает в себя:

- настройка общих параметров;
- назначение ролей субъектам доступа;
- настройка конфигурации на автономных клиентах — включает редактирование параметров сканирования, импорт настроек со съемного машинного носителя (СМН).

Раздел привилегий «Работа с Проектом паспорта ПО, Паспортом ПО» включает в себя:

- просмотр Проекта паспорта ПО, Паспорта ПО;
- выполнение сравнения Проекта паспорта ПО с Паспортом ПО, Паспортов ПО между собой;
- выполнение сканирования по команде из Консоли СК;
- выполнение сканирования по команде в автономном режиме клиента;
- утверждение Проекта паспорта ПО с помощью ПЭП;
- удаление из БД СК Паспорта ПО;
- загрузка Проекта паспорта ПО с СМН на СК;
- экспорт СПС (Проект паспорта ПО) на СМН (для автономных клиентов);
- импорт заверенного Проекта паспорта ПО с СМН (для автономных клиентов).

Для групп установлены следующие привилегии (таблица 1):

Таблица 1. Список привилегий, выставленных по умолчанию

Группа	Группа привилегий	Набор привилегий по умолчанию
Аудитор	Администрирование	Нет привилегий
	Работа с учетными записями, группами, ролями	Нет привилегий
	Настройка параметров	Нет привилегий
	Работа с Проектом паспорта ПО, Паспортом ПО	Просмотр Проекта паспорта ПО, Паспорта ПО
		Выполнение сравнения Проекта паспорта ПО с Паспортом ПО, Паспортов ПО между собой

Группа	Группа привилегий	Набор привилегий по умолчанию
		Выполнение сканирования по команде в автономном режиме клиента
		Экспорт СПС (Проект паспорта ПО) на СМН (с автономного клиента)
		Импорт заверенного Проекта паспорта ПО с СМН (для автономного клиента)
Контролер	Администрирование	Просмотр журнала
	Работа с учетными записями, группами, ролями	Просмотр свойств учетной записи или группы учетных записей
	Настройка параметров	Нет привилегий
	Работа с Проектом паспорта ПО, Паспортом ПО	Выполнение сканирования по команде из Консоли СК
		Утверждение Проекта паспорта ПО с помощью ЭП
		Загрузка Проекта паспорта ПО с СМН в СК (для автономных клиентов)
		Проверка Паспорта ПО
		Все полномочия Аудитора
Администратор СК	Администрирование	Формирование списка контролируемых ПК
		Формирование групп ПК
		Выполнение операций над клиентами
		Просмотр журнала
		Настройка детальности регистрируемых событий
	Работа с учетными записями, группами, ролями	Управление учетными записями и группами учетных записей
	Настройка параметров	Настройка общих параметров
		Назначение ролей субъектам доступа
	Работа с Проектом паспорта ПО, Паспортом ПО	Удаление Паспорта ПО
		Все полномочия Контролера
Администратор ИБ	Администрирование	Все полномочия Администратора СК
	Работа с учетными записями, группами, ролями	Назначение Администратора СК
		Создание учетных записей пользователей и групп на автономных ПК и назначение им ролей
		Все полномочия Администратора СК
	Настройка параметров	Настройка параметров сканирования автономных клиентов
		Все полномочия Администратора СК
	Работа с Проектом паспорта ПО, Паспортом ПО	Выполнение сканирования по команде в автономном режиме клиента
		Экспорт СПС (Проект паспорта ПО) на СМН (с автономного клиента)
		Импорт заверенного Проекта паспорта ПО с СМН (для автономного клиента)
		Все полномочия Администратора СК

3.4 Работа с категорией «Паспорт ПО»

При переходе в категорию «Паспорт ПО» открывается соответствующая панель инструментов

(Рис. 22).

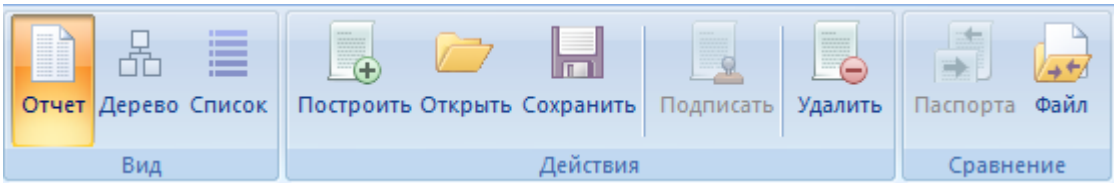


Рис. 22. Панель инструментов категории «Паспорт ПО»

На уровне СК и группы клиентов вывод данных по сформированным Проектам паспортов ПО и подписанным Паспортам ПО не выполняется, рабочая область имеет вид, отраженный на Рис. 12. Область информации о клиентах СК отражает:

- общее количество нарушений (расхождений между данными сформированного Проекта паспорта ПО и утвержденного Паспорта ПО в рамках клиентского ПК);
- общее число клиентов, с которыми не устанавливается связь;
- общее число подключенных клиентов с отсутствующими нарушениями;
- общее число отключенных клиентов;
- общее число не активированных клиентов;
- общее число клиентов.

Просмотр сформированного Проекта паспорта ПО и всех Паспортов ПО выполняется только на уровне клиента. При открытии категории Паспорт ПО в списке всех Паспортов ПО выполняется вывод:

- Проект паспорта ПО,
- Паспорт ПО,
- все сохраненные Паспорта ПО для данного клиента (Рис. 23).

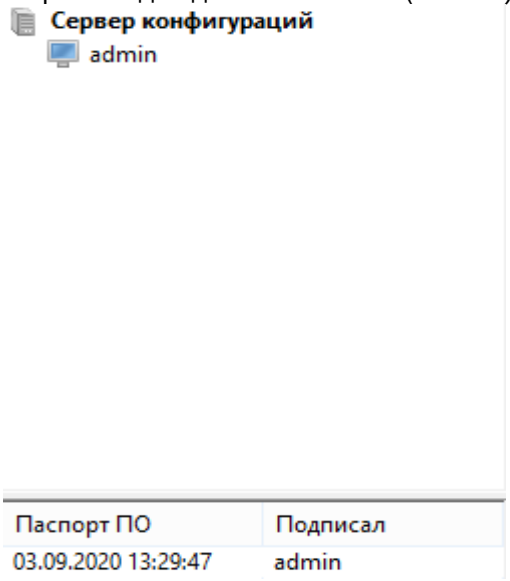


Рис. 23. Сохраненные Паспорта ПО для клиента

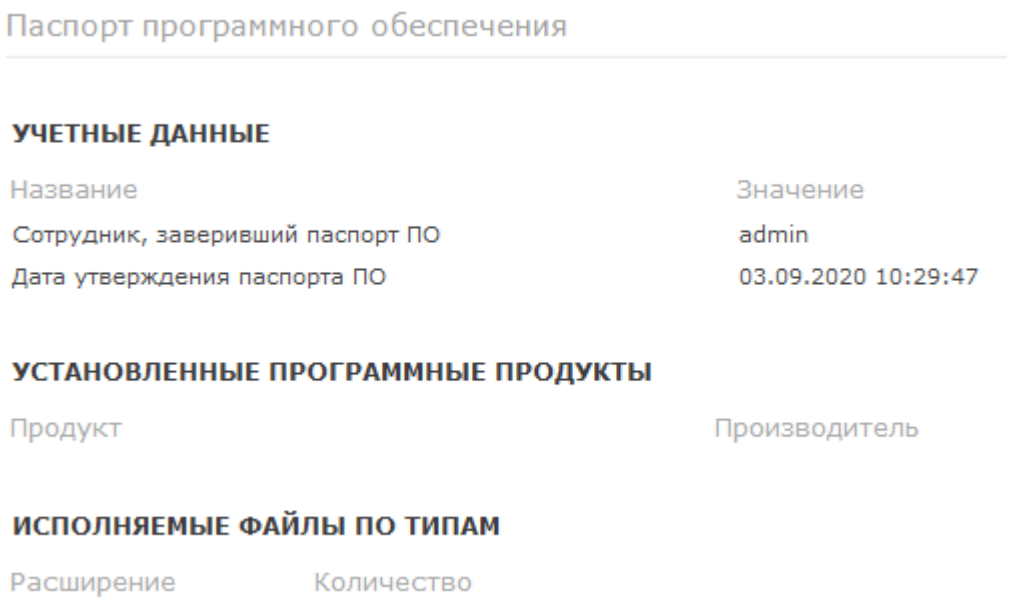
Для каждого Проекта паспорта ПО и Паспорта ПО в списке выполняется вывод следующих данных:

- для Проекта паспорта ПО — дата и время формирования, для Паспорта ПО — дата и время утверждения;
- для Паспорта ПО — логин пользователя, который утвердил Паспорт ПО, для Проекта паспорта ПО — прочерк «-».

Рабочая область — окно вывода данных выбранного Паспорта ПО либо Проекта паспорта ПО. По умолчанию выполняется вывод данных действующего Паспорта ПО.

При выборе на панели инструментов вида «Отчет» в рабочей области выводится «Паспорт ПО», содержащий следующую информацию (Рис. 24):

- учетные данные;
- установленные программные продукты (с указанием наименования и производителя продукта);
- исполняемые файлы по типам (с указанием расширения и количества).


Паспорт программного обеспечения

УЧЕТНЫЕ ДАННЫЕ

Название	Значение
Сотрудник, заверивший паспорт ПО	admin
Дата утверждения паспорта ПО	03.09.2020 10:29:47

УСТАНОВЛЕННЫЕ ПРОГРАММНЫЕ ПРОДУКТЫ

Продукт	Производитель

ИСПОЛНЯЕМЫЕ ФАЙЛЫ ПО ТИПАМ

Расширение	Количество

Рис. 24. Сведения из раздела «Паспорт ПО»

Для просмотра выбранного Паспорта ПО либо Проекта паспорта ПО в виде дерева объектов используется команда «Дерево» на панели «Вид». Паспорт ПО либо Проект паспорта ПО представляется в формате дерева объектов, соответствующего структуре каталогов ПК, и списка файлов с параметрами (таблица 2).

Для просмотра выбранного Паспорта ПО либо Проекта паспорта ПО в виде списка предназначена команда «Список» на панели «Вид». Паспорт ПО либо Проект паспорта ПО представляется в формате списка контролируемых файлов. Сортировка файлов выполняется по любому из полей (таблица 2).

Таблица 2. Список отображаемых параметров

Параметр	Поле	Отображение по умолчанию
Полный путь к файлу (с указанным расширением)	Имя файла	+
Версия файла	Версия файла	+
Разработчик (название организации, которая является создателем файла)	Разработчик	+
Продукт	Продукт	+
Дата и время модификации файла	Последнее изменение	+
Длина файла (объем файла в КБ)	Длина файла	+
Значение хэш-функции файла (контрольная сумма)	Подпись файла	+

Для формирования Проекта паспорта ПО необходимо выполнить сканирование клиента и выбрать команду «Построить».

Если во время выполнения сканирования была выполнена перезагрузка клиента в штатном режиме, то при возобновлении работы сканирование перезапускается, в журнал клиента заносится ошибка «Операция прервана пользователем», в журнал СК заносится запись «Выполнение сканирования на клиенте было прервано. Сканирование запущено заново».

Если во время выполнения сканирования произошел обрыв связи, то при возобновлении работы клиент сообщает СК результаты последнего сканирования.

Если во время выполнения сканирования СК отключил сканирование для данного клиента, то клиент прекращает сканирование, в журнал клиента заносится ошибка «Операция прервана сервером».

Если для клиента был сформирован Проект паспорта ПО, то после выполнения сканирования он заменяется новым, поскольку Проект паспорта ПО может быть только один.

После выполнения сканирования автоматически выполняется сравнение полученных данных с данными действующего Паспорта ПО, в случае выявления различий в данных состояние клиента в

дереве объектов изменяется на «Нарушение».

Автоматически выполняется контроль отсутствия модификации подписанного Паспорта ПО (результат проверки фиксируется в поле «Верификация подписи»).

Команда «Открыть» предназначена для импорта файла:

- в качестве файла может быть использован файл с данными Проекта паспорта ПО или файл с данными Паспорта ПО в формате XML;
- при выборе команды открывается диалоговое окно, где необходимо указать полный путь к файлу;
- если выполняется загрузка Проекта паспорта ПО и для данного клиента уже был сформирован Проект с более ранней датой формирования, то происходит замена на новый;
- если выполняется загрузка Проекта паспорта ПО с более ранней датой формирования, чем сохраненный для данного клиента Проект, выводится информационное сообщение, что выполняется загрузка Проекта с более ранней датой формирования, необходимо подтвердить замену Проекта паспорта ПО;
- при загрузке Паспорта ПО, автоматически выполняется контроль отсутствия модификации подписанного файла;
- после выполнения команды «Подписать» Проект паспорта ПО сохраняется в БД СК.

Для сохранения Паспорта ПО в формат XML (с расширением .pass) необходимо при выборе Проекта паспорта ПО либо Паспорта ПО в общем списке Паспортов ПО клиента и вызвать команду «Сохранить», выбрать каталог сохранения файла в открывшемся окне. Далее есть возможность загрузить новый Паспорт ПО непосредственно на клиенте, который находится в автономном режиме управления.

Команда «Удалить» предназначена для удаления выбранных Паспортов ПО в общем списке клиента:

- можно выполнить удаление Проекта паспорта ПО либо недействующих Паспортов ПО, удаление действующего Паспорт ПО невозможно;
- выбор удаляемого объекта (объектов) выполняется с помощью выбора необходимой строки (строк) в общем списке.

Команда «Подписать» позволяет заверить ПЭП действующий Проект паспорта ПО. Для двух различных Паспортов ПО гарантируется различная подпись.

Заверенный Проект паспорта ПО становится действующим Паспортом ПО для выбранного клиента. Если был утвержден новый Паспорт ПО, то на клиенте выполняется замена Паспорта ПО.

После подписания Проекта паспорта ПО в случае, когда состояние клиента в дереве объектов было «Нарушение», состояние клиента в дереве объектов обновляется.

Команды раздела «Сравнение» предназначены для выполнения сравнения двух выбранных файлов в общем списке Паспортов ПО клиента или сравнения выбранного Паспорта ПО с файлом.

При выборе в общем списке Паспортов ПО единственной строки, активна только команда «Файл», позволяющая сравнить выбранный Паспорт ПО с файлом (при выборе команды открывается диалоговое окно, в котором необходимо указать путь к файлу, с которым необходимо выполнить сравнение).

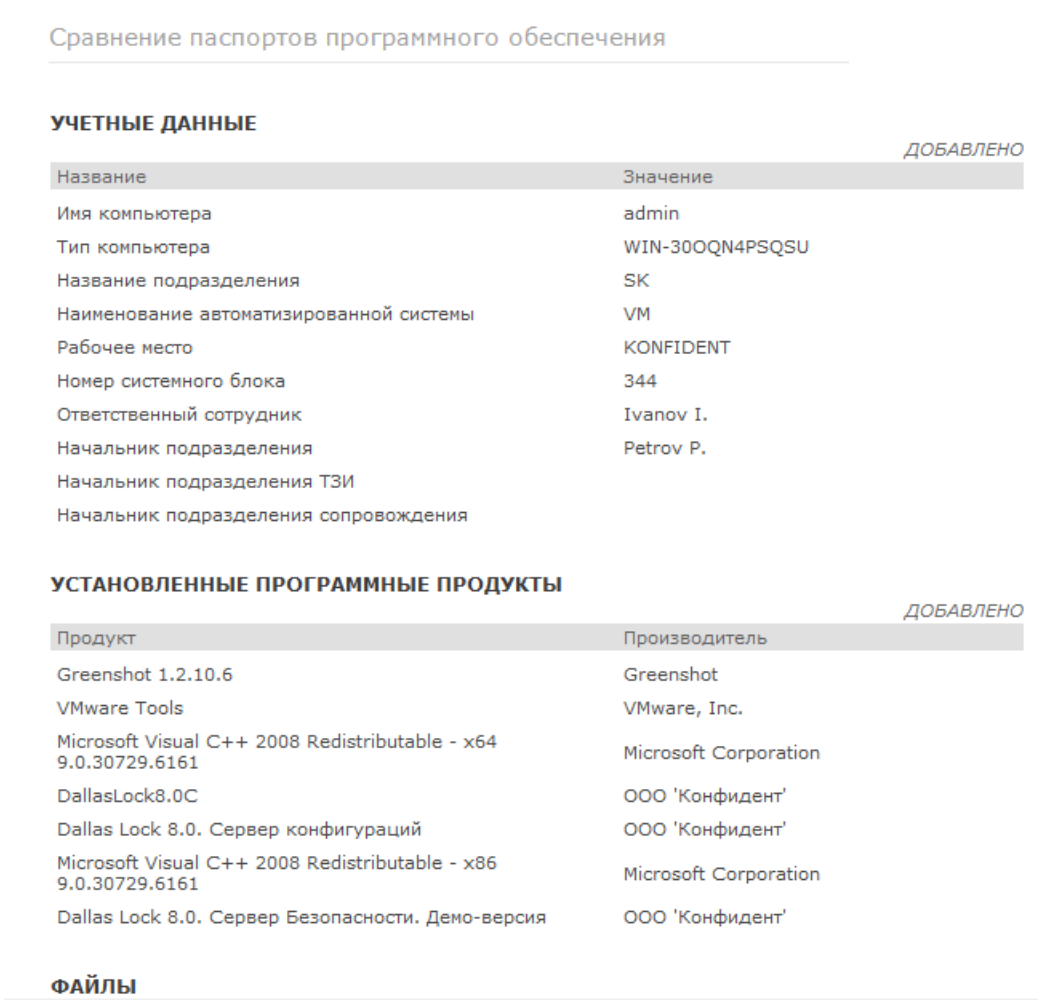
При выборе в общем списке двух строк (выделение нескольких строк возможно при зажатой клавише «Ctrl») становится активной команда «Паспорта» (команда «Файл» при этом становится неактивной), которая выполняет сравнение двух выбранных Паспортов ПО из общего списка.

При выборе в общем списке более двух строк команды «Паспорта» и «Файл» неактивны.

При выполнении сравнения автоматически выполняется контроль отсутствия модификации подписанного файла, результат проверки фиксируется в поле «Подпись верна» учетных данных.

После выполнения сравнения в рабочей области отображается результат выполненного сравнения, который содержит (Рис. 25):

- данные по файлам в соответствии с таблицей 2
- статус соответствия по каждому измененному файлу (новый, удален, изменен);
- наименование сравниваемых объектов.



Сравнение паспортов программного обеспечения

УЧЕТНЫЕ ДАННЫЕ

ДОБАВЛЕНО

Название	Значение
Имя компьютера	admin
Тип компьютера	WIN-30OQN4PSQSU
Название подразделения	SK
Наименование автоматизированной системы	VM
Рабочее место	KONFIDENT
Номер системного блока	344
Ответственный сотрудник	Ivanov I.
Начальник подразделения	Petrov P.
Начальник подразделения ТЗИ	
Начальник подразделения сопровождения	

УСТАНОВЛЕННЫЕ ПРОГРАММНЫЕ ПРОДУКТЫ

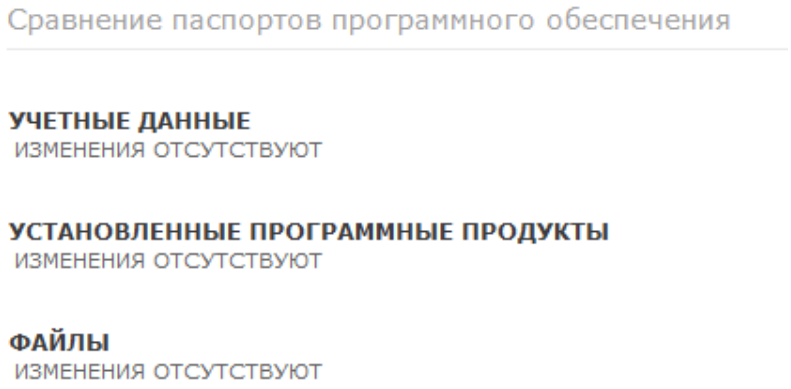
ДОБАВЛЕНО

Продукт	Производитель
Greenshot 1.2.10.6	Greenshot
VMware Tools	VMware, Inc.
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161	Microsoft Corporation
DallasLock8.0C	ООО 'Конфидент'
Dallas Lock 8.0. Сервер конфигураций	ООО 'Конфидент'
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161	Microsoft Corporation
Dallas Lock 8.0. Сервер Безопасности. Демо-версия	ООО 'Конфидент'

ФАЙЛЫ

Рис. 25. Сравнение разных Паспортов ПО

Если выбраны Паспорта ПО или Проекты паспорта ПО, между которыми нет разницы, сравнение покажет, что изменения отсутствуют (Рис. 26).



Сравнение паспортов программного обеспечения

УЧЕТНЫЕ ДАННЫЕ
ИЗМЕНЕНИЯ ОТСУТСТВУЮТ

УСТАНОВЛЕННЫЕ ПРОГРАММНЫЕ ПРОДУКТЫ
ИЗМЕНЕНИЯ ОТСУТСТВУЮТ

ФАЙЛЫ
ИЗМЕНЕНИЯ ОТСУТСТВУЮТ

Рис. 26. Сравнение не имеющих отличий Паспортов ПО

3.5 Работа с категорией «Учетные записи»

В рамках СК возможно управление учетными записями ДБ. Настройка списка доменных учетных записей осуществляется в категории «Учетные записи», при переходе в которую открывается соответствующая панель инструментов (Рис. 27).

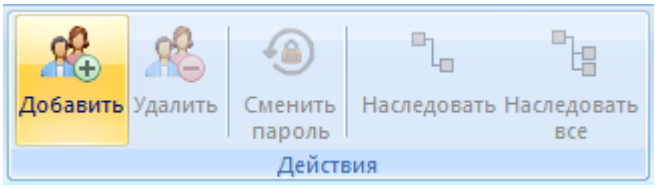


Рис. 27. Панель инструментов категории «Учетные записи»

Рабочая область категории «Учетные записи» состоит из списка учетных записей с назначенными им группами (Рис. 28):

- Админ. ИБ,
- Админ. СК,
- Контролер,
- Аудитор,
- Отключен.

Логин	Имя	Админ. ИБ	Админ. СК	Контролер	Аудитор	Отключен
admin	Администратор	◉	○	○	○	○
secServ	secServ	○	◉	○	○	○

Рис. 28. Рабочая область категории «Учетные записи»

При использовании БД СБ DL список учетных записей в СК формируется на основании списка БД СБ, список учетных записей в этом случае открыт в режиме чтения. Добавление новой учетной записи, отключение и включение учетной записи выполняется только из Консоли СБ DL.

При использовании собственной БД администратору СК необходимо самостоятельно сформировать список учетных записей, то есть необходимо продублировать создание учетной записи в СБ DL и заполнить для нее необходимые параметры.

По умолчанию в списке учетных записей зарегистрирована учетная запись Администратора ИБ, которая была создана при установке СК. Данная учетная запись системна и не может просматриваться, редактироваться, удаляться.

Создание учетной записи (функциональная возможность доступна только при использовании собственной БД) выполняется на уровне СК.

Для создания учетной записи необходимо выбрать команду «Добавить» на панели «Действия», в списке появится новая строка с возможностью редактирования поля «Логин» (обязательно для заполнения) и «Имя» и с возможностью выбрать группу. Чтобы подтвердить создание учетной записи, необходимо нажать на клавишу Enter либо щелкнуть левой кнопки мыши.

Учетная запись создается глобально на уровне всего ДБ и далее администратор СК определяет для какого клиента и группы клиентов включить либо отключить данную учетную запись (отключение учетной записи для группы и клиента выполняется с помощью установки переключателя «Отключен», если переключатель не установлен, то учетная запись включена). Первоначально при регистрации учетная запись отключена. Учетная запись может быть включена для группы, но отключена для конкретного клиента, входящего в состав данной группы.

Редактирование параметров учетной записи «Логин» и «Имя» выполняется непосредственно в строке с данными (функциональная возможность недоступна при использовании БД СБ DL).

Удаление учетной записи (функциональная возможность доступна только при использовании собственной БД) выполняется на уровне СК. Для удаления необходимо выбрать в общем списке учетную запись или группу учетных записей и выполнить команду «Удалить» на панели «Действия», после чего подтвердить свое действие в появившемся окне подтверждения удаления.

Назначение группы для учетной записи выполняется следующим образом:

- в общем списке выбирается учетная запись и для данной учетной записи с помощью переключателя выполняется выбор группы;
- при первоначальной регистрации учетной записи для нее автоматически выставляется значение группы «Аудитор»;
- если группа настраиваются глобально на уровне СК, то для остальных уровней параметры наследуются или переопределяются на уровне конкретного клиента или группы клиентов;
- в общем списке автоматически будет добавлена учетная запись с группой «Администратор ИБ» (учетная запись пользователя, под которой был установлен СК);

- для учетной записи пользователя может быть назначена только одна группа;
- группа «Администратор ИБ», как и другие, может быть включена для нескольких пользователей;
- переопределение групп на уровне клиента и группы клиентов выполняется при переходе на необходимый уровень дерева объектов, выбора нужной учетной записи и переключением группы.

3.6 Работа с категорией «Настройки»

Настройка глобальных параметров выполняется на уровне СК категории «Настройки», при переходе в которую открывается соответствующая панель инструментов (Рис. 29).

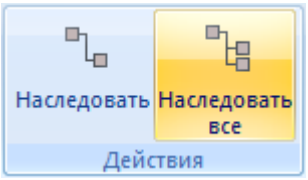


Рис. 29. Панель инструментов категории «Учетные записи»

Общие параметры настраиваются глобально и наследуются для дочерних объектов. Параметры могут быть переопределены для выбранного объекта. Значения параметров могут быть переопределены только на уровне родительского объекта, редактирование значений параметров не выполняется на уровне клиента.

«Расписание/периодичность сканирования» позволяет установить расписание/периодичность выполнения сканирования. По умолчанию для параметра выставлено пустое значение. При редактировании параметра (двойной щелчок мыши) открывается форма настройки расписания и периодичности сканирования (Рис. 30). При нажатии стрелки напротив значения «Ежедневно» можно выбрать значение параметра период сканирования из выпадающего списка, в котором перечислены возможные варианты настройки периодов: ежедневно, 1 раз в 2 дня, 1 раз в 3 дня, 1 раз в 5 дней, еженедельно, 1 раз в 2 недели, ежемесячно. Настройка расписания сканирования выполняется аналогично настройке расписания синхронизации в Консоли СБ.

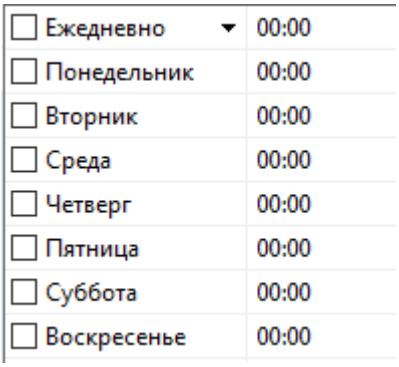


Рис. 30. Форма настройки расписания/периодичности сканирования

«Исключить каталоги и файлы» предназначен для исключения локальных дисков ПК, каталогов, файлов из области сканирования. По умолчанию выставлено пустое значение, то есть выполняется сканирование всех локальных дисков, каталогов, файлов. Для добавления исключения необходимо в строке значения ввести наименование исключаемых дисков, каталогов, файлов через точку с запятой.

«Расширения сканируемых файлов» позволяет добавить либо удалить из области сканирования файлы по расширениям. По умолчанию в значении параметра указаны следующие расширения: exe; com; dll; ocx; cmd; bat; vb; vbs; vbe; cpl; scr; drv; sys; js; jse; jar; ps1; wsf; msi; msu; bpl; ppl; ovl. Для добавления необходимо в строке значения ввести дополнительные расширения через точку с запятой, для удаления — удалить наименование расширения непосредственно в поле значения.

Если значения параметров для группы клиентов наследуются, то они выделены серым шрифтом. Если значения параметров были переназначены, то они выделяются черным шрифтом.

Для переопределения значения параметра на уровне группы клиентов необходимо выбрать соответствующий параметр и выполнить его редактирование, после редактирования данный параметр выделяется черным шрифтом.

Команда «Наследовать» позволяет установить наследование значения параметра от родительского объекта для выбранного объекта — после выполнения команды выбранный

параметр наследует значение от родительского объекта и выделяются серым шрифтом.

Команда «Наследовать все» позволяет установить наследование значений для всех параметров от родительского объекта для выбранного объекта — после выполнения команды все параметры для объекта наследуют значения от родительского объекта и выделяются серым шрифтом.

При обращении клиента к серверу (подключается при запуске и постоянно подключен к серверу) клиент обновляет параметры в соответствии с теми, что были выставлены на сервере.

Категория «Настройки» на уровне клиента дополнительно содержит в рабочей области параметры (Рис. 31):

- Имя компьютера,
- Тип компьютера,
- Название подразделения,
- Наименование автоматизированной системы,
- Рабочее место,
- Номер системного блока,
- Ответственный сотрудник,
- Начальник подразделения,
- Начальник подразделения ТЗИ,
- Начальник подразделения сопровождения.

Параметр	Значение
Имя компьютера	admin
Тип компьютера	WIN-30OQN4PSQSU
Название подразделения	SK
Наименование автоматизированной системы	VM
Рабочее место	KONFIDENT
Номер системного блока	344
Ответственный сотрудник	Ivanov I.
Начальник подразделения	Petrov P.
Начальник подразделения ТЗИ	
Начальник подразделения сопровождения	
Параметры сканирования	
Расписание/периодичность сканирования	Ежедневно, 00:00;
Исключить каталоги и файлы	
Расширения сканируемых файлов	exe;com;dll;ocx;cmd;bat;vb;vbs;vbe;cpl;scr;drv;sys;js;jse;jar;ps1;wsf;msi;msu;bpl;ppl;ovl

Рис. 31. Рабочая область категории «Настройки»

3.7 Работа с категорией «Журнал»

События серверной и клиентской части СК регистрируются в журнале СК. Просмотр событий журнала выполняется в категории «Журнал».

При переходе в категорию «Журнал» открывается соответствующая панель инструментов, включающая в себя категорию «Действия» (Рис. 32).

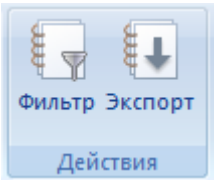


Рис. 32. Панель инструментов категории «Журнал»

С клиента выполняется сбор журнала управления политиками, в котором отображаются только события, касающиеся модуля конфигурации, список событий для клиента указан в таблице 3. При появлении нового события клиентская часть передает это событие серверу.

На уровне СК выполняется просмотр событий для всех клиентов, в том числе и для серверной части. На уровне группы — список событий клиентов, входящих в состав данной группы, на уровне клиента — только для выбранного клиента.

В журнале выводятся следующие поля (сортировка может выполняться пользователем по любому из полей) представленные на Рис. 33:

- ID — идентификатор события;
- Время — дата и время события;

- Клиент — идентификатор компьютера: если событие касается клиентского ПК, то фиксируется наименованием данного клиентского ПК, если событие касается СК, то фиксируется имя ПК, на котором установлен СК;
- Пользователь — логин учетной записи пользователя, которым было инициировано событие;
- Событие — тип события;
- Дополнительно — вывод дополнительной информации по событию;
- Результат — результат выполнения события.

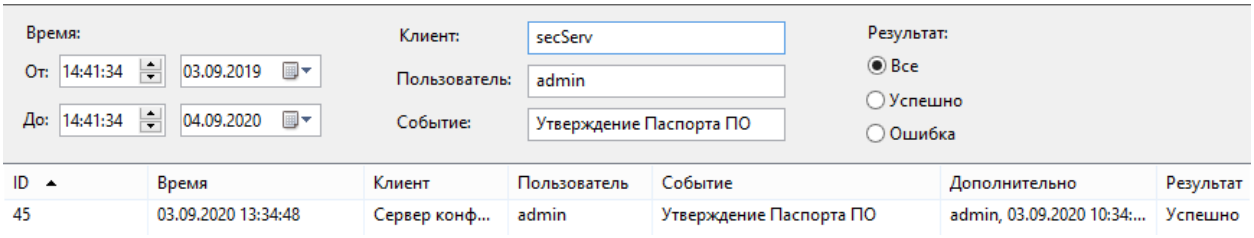


Рис. 33. Категория «Журнал»

Таблица 3. Список событий СК

№	Тип события	Обязательные к регистрации данные	Момент добавления
1	Утверждение Паспорта ПО	• Идентификатор события (поле ID); • дата и время события (поле «Время»); • идентификатор компьютера (поле «Клиент»); • идентификатор Паспорта ПО (поле «Дополнительно»); • идентификатор пользователя (поле «Пользователь»); • результат (поле «Результат»): Успешно либо Ошибка (описание ошибки)	После выполнения команды «Подписать» панели «Действия» вкладки «Паспорт ПО»
2	Удаление Паспорта ПО	• Идентификатор события (поле ID); • дата и время события (поле «Время»); • идентификатор компьютера (поле «Клиент»); • идентификатор Паспорта ПО (поле «Дополнительно»); • идентификатор пользователя (поле «Пользователь»); • результат (поле «Результат»): Успешно либо Ошибка (описание ошибки)	После выполнения команды «Удалить» панели «Действия» вкладки «Паспорт ПО»
3	Загрузка Проекта паспорта ПО	• Идентификатор события (поле ID); • дата и время события (поле «Время»); • идентификатор компьютера (поле «Клиент»); • идентификатор Паспорта ПО (поле «Дополнительно»); • идентификатор пользователя (поле «Пользователь»); • результат (поле «Результат»): Успешно либо Ошибка (описание ошибки)	После выполнения команды «Открыть» для Проекта паспорта ПО панели «Действия» вкладки «Паспорт ПО»
4	Синхронизация Паспортов ПО клиента	• Идентификатор события (поле ID); • дата и время события (поле «Время»); • идентификатор компьютера (поле «Клиент»); • идентификатор Паспорта ПО (поле «Дополнительно»); • идентификатор пользователя (поле «Пользователь»); • результат (поле «Результат»): Успешно либо Ошибка (описание ошибки)	После выполнения синхронизации Паспортов ПО между клиентом и сервером (в момент обращения клиента к серверу)
5	Сканирование	• идентификатор события (поле ID);	По завершению

№	Тип события	Обязательные к регистрации данные	Момент добавления
		• дата и время события (поле «Время»); • идентификатор компьютера (поле «Клиент»); • идентификатор пользователя (поле «Пользователь»); • результат (поле «Результат»): Выполнено, Ошибка; Описание ошибки: этап, на котором выявлена ошибка; имя файла или каталога, при доступе к которому произошел сбой, или пустая строка, если произошла другая ошибка, не связанная с доступом; описание реакции на ошибку (сбор данных продолжается, сбор данных остановлен)	сканирования по команде пользователя (по команде «Построить») или в соответствии с установленным расписанием/периодом
6	Редактирование параметров	• Идентификатор события (поле ID); • дата и время события (поле «Время»); • идентификатор компьютера (поле «Клиент»): имя ПК СК; • идентификатор пользователя (поле «Пользователь»); • результат (поле «Результат»): Успешно либо Ошибка (описание ошибки)	После выполнения редактирования любого параметра
7	Включить сканирование	• Идентификатор события (поле ID); • дата и время события (поле «Время»); • идентификатор компьютера (поле «Клиент»): имя клиентского ПК, для которого включили модуль; • идентификатор пользователя (поле «Пользователь»); • результат (поле «Результат»): Успешно либо Ошибка (описание ошибки)	После выполнения команды «Включить сканирование» для выбранного клиента в дереве объектов и получение ответа от клиента, что модуль включен
8	Отключить сканирование	• Идентификатор события (поле ID); • дата и время события (поле «Время»); • идентификатор компьютера (поле «Клиент»): имя клиентского ПК, для которого отключили модуль; • идентификатор пользователя (поле «Пользователь»); • результат (поле «Результат»): Успешно либо Ошибка (описание ошибки)	После выполнения команды «Отключить сканирование» для выбранного клиента, который выполнял сканирование в дереве объектов и получение ответа от клиента, что модуль отключен
9	Подключение к СБ DL	• Идентификатор события (поле ID); • дата и время события (поле «Время»); • идентификатор компьютера (поле «Клиент»): имя ПК СК; • идентификатор пользователя (поле «Пользователь»); • результат (поле «Результат»): Ошибка (описание ошибки «Не удалось подключиться к СБ DL»)	Событие фиксируется, если произошла ошибка при обращении к СБ DL
10	Добавление учетной записи	• Идентификатор события (поле ID); • дата и время события (поле «Время»); • идентификатор компьютера (поле «Клиент»): имя ПК СК; • наименование учетной записи (поле «Дополнительно»); • идентификатор пользователя (поле «Пользователь»); • результат (поле «Результат»): Успешно либо Ошибка (описание ошибки)	Событие фиксируется, если на СБ DL была добавлена новая учетная запись и данная учетная запись была добавлена в БД СК

№	Тип события	Обязательные к регистрации данные	Момент добавления
11	Удаление учетной записи	• Идентификатор события (поле ID); • дата и время события (поле «Время»); • идентификатор компьютера (поле «Клиент»): имя ПК СК; • наименование учетной записи (поле «Дополнительно»); • идентификатор пользователя (поле «Пользователь»); • результат (поле «Результат»): Успешно либо Ошибка (описание ошибки)	Событие фиксируется в случае, если на СБ DL была удалена учетная запись и данная учетная запись была удалена в БД СК
12	Редактирование учетной записи	• Идентификатор события (поле ID); • дата и время события (поле «Время»); • идентификатор компьютера (поле «Клиент»): имя ПК СК; • наименование учетной записи (поле «Дополнительно»); • идентификатор пользователя (поле «Пользователь»); • результат (поле «Результат»): Успешно либо Ошибка (описание ошибки)	Событие фиксируется в случае, если на СБ DL было выполнено редактирование учетной записи и данные изменения были внесены в БД СК
13	Добавление клиента	• Идентификатор события (поле ID); • дата и время события (поле «Время»); • наименование клиента (поле «Клиент»): имя ПК СК; • идентификатор Паспорта ПО (поле «Дополнительно»); • идентификатор пользователя (поле «Пользователь»); • результат (поле «Результат»): Успешно либо Ошибка (описание ошибки)	Событие фиксируется в случае, если на СБ DL был добавлен новый клиент и данный клиент был добавлен в БД СК
14	Удаление клиента	• Идентификатор события (поле ID); • дата и время события (поле «Время»); • идентификатор компьютера (поле «Клиент»): имя ПК СК; • наименование клиента (поле «Дополнительно»); • идентификатор пользователя (поле «Пользователь»); • результат (поле «Результат»): Успешно либо Ошибка (описание ошибки)	Событие фиксируется в случае, если на СБ DL был удален клиент и данный клиент был удален в БД СК
15	Перемещение клиента	• Идентификатор события (поле ID); • дата и время события (поле «Время»); • идентификатор компьютера (поле «Клиент»): имя ПК СК; • наименование клиента (поле «Дополнительно»); • идентификатор пользователя (поле «Пользователь»); • результат (поле «Результат»): Успешно либо Ошибка (описание ошибки)	Событие фиксируется в случае, если на СБ DL было выполнено перемещение клиента и данные изменения были внесены в БД СК

На панели «Действия» доступны следующие команды:

- «Фильтр» — команда настройки фильтра журнала, которая позволяет выполнять настройку фильтра по столбцам «Время», «Клиент», «Пользователь», «Результат», «Событие» (Рис. 34).

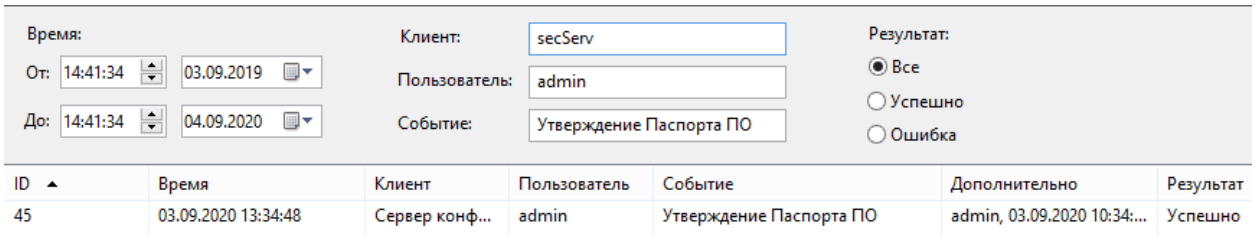


Рис. 34. Настройка фильтра журнала

- «Экспорт» — команда экспорта всего журнала или отфильтрованных записей, данные могут быть загружены на устройство в форматах TXT и XML. Загруженные данные имеют вид: идентификатор события; дата и время события; идентификатор компьютера; идентификатор пользователя; событие; дополнительно (Рис. 35).

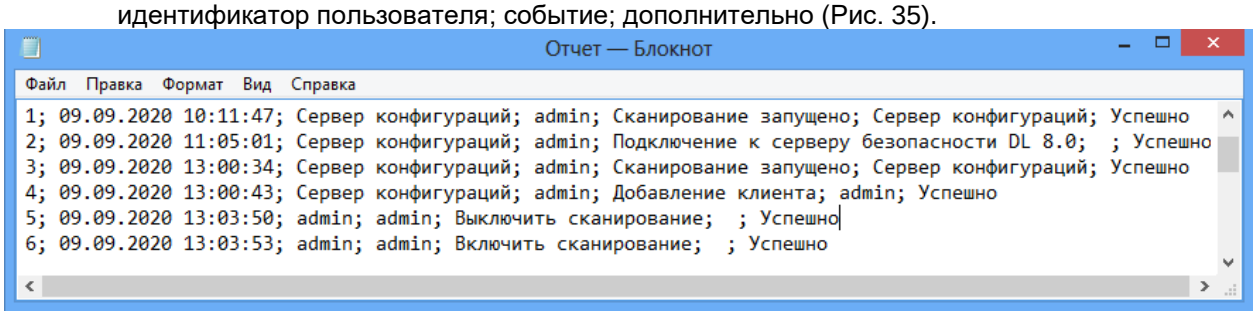


Рис. 35. Вид экспортируемых данных из журнала

4 РАБОТА КЛИЕНТСКОЙ ЧАСТИ СЕРВЕРА КОНФИГУРАЦИЙ

4.1 Основы работы

Клиент осуществляет сбор и передачу информации о СПС на СК. Клиентская часть обеспечивает информационное взаимодействие как в режиме централизованного управления, так и в автономном режиме.

В изделии реализована функция фиксации событий подсистемы сканирования клиентской части в журнале СК. Фиксируются следующие типы событий:

- сканирование,
- редактирование параметров,
- загрузка Паспорта ПО с СМН,
- синхронизация Паспортов ПО клиента.

Основные функциональные возможности клиента:

- сбор информации о СПС, формирование Проекта паспорта ПО;
- передача серверу сведений о СПС, отслеживание изменений в установленном ПО на клиентах;
- прием от сервера заверенного Проекта паспорта ПО;
- просмотр Проекта паспорта ПО;
- просмотр утвержденных Паспортов ПО;
- сравнение Паспортов ПО между собой;
- сравнение Проекта паспорта ПО и утвержденного Паспорта ПО;
- настройка конфигурационных данных сканирования;
- выгрузка Проекта паспорта ПО с автономного клиента;
- загрузка утвержденного Паспорта ПО с сервера в БД автономного клиента.

4.2 Паспорт программного обеспечения

Просмотр, анализ, настройка конфигурационных параметров клиента выполняется в разделе: «Отчет» → «Паспорт программного обеспечения» основного меню ОА. Панель инструментов имеет 4 раздела (Рис. 36):

- Категории. Включает команды: «Паспорт», «Проект паспорта», «Настройки».
- Вид. Включает команды: «Отчет», «Дерево», «Список».
- Действия. Включает команды: «Построить», «Открыть», «Сохранить как», «Применить», «Удалить».
- Сравнение. Включает команды: «Паспорт», «Файл».

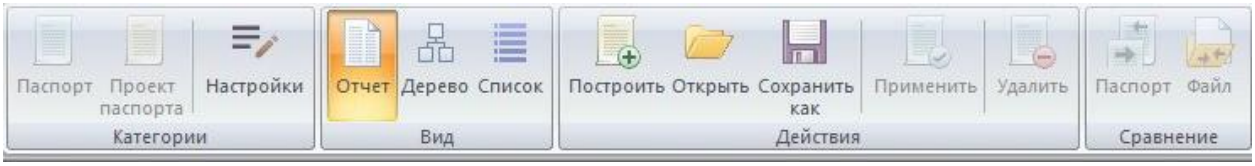


Рис. 36. Панель инструментов

Панель быстрого доступа может быть дополнительно настроена по аналогии с панелью серверной части (см. раздел Основы работы).

При вызове команды «Паспорт» по умолчанию в рабочей области формы открывается действующий Паспорт ПО (последний по дате утверждения Паспорт ПО).

Если файла с Паспортом ПО на ПК нет, то открывается Проект паспорта ПО. Если Паспорт ПО и Проект паспорта ПО не были сформированы на клиенте, то пользователю необходимо построить Проект паспорта ПО (будет выведено соответствующее информационное сообщение).

Паспорт ПО имеет вид, описанный в разделе Работа с категорией «Паспорт ПО».

Если в процессе выполнения сканирования произошла ошибка в процессе доступа к какому-либо файлу или каталогу, то сканирование продолжается, в Проекте паспорта ПО в поле «Контрольная сумма» для данного ресурса указывается «Отказано в доступе». В журнале управления политиками фиксируется соответствующее событие.

Если в процессе выполнения сканирования произошла ошибка, влияющая на работоспособность системы в целом, и дальнейшее выполнение сбора данных не является возможным, то сканирование прерывается, Проект паспорта ПО не формируется. В журнале управления политиками фиксируется соответствующее событие.

Для просмотра выбранного Паспорта ПО либо Проекта паспорта ПО в виде дерева объектов используется команда «Дерево» на панели «Вид». Паспорт ПО либо Проект паспорта ПО представляется в формате дерева объектов, соответствующего структуре каталогов ПК, и списка файлов с параметрами (таблица 2).

Для просмотра выбранного Паспорта ПО либо Проекта паспорта ПО в виде списка предназначена команда «Список» на панели «Вид». Паспорт ПО либо Проект паспорта ПО представляется в формате списка контролируемых файлов. Сортировка файлов выполняется по любому из полей (таблица 2). Команда «Паспорт» позволяет вернуться к формату просмотра данных в виде Паспорта ПО.

Сохранение отчета Проекта паспорта ПО выполняется с помощью команды «Сохранить как». Доступны следующие форматы:

- оптимальная для печати — Паспорт ПО будет сохранен в формате RTF без подробной информации по каждому файлу;
- полная — Паспорт ПО будет сохранен в формате TXT в полном виде с подробной информацией по каждому файлу.

Сохранение отчета Проекта паспорта ПО выполняется для сохранения данных сканирования на клиентском ПК.

Если Проект паспорта ПО не был предварительно сохранен и пользователь выбирает любую другую команду, то Проект паспорта ПО сохраняется автоматически в каталог C:\DLLOCK80\Passports в формате XML (с расширением .pass).

Для просмотра ранее сохраненного или стороннего Проекта Паспорта ПО, загруженного с СМН, необходимо выполнить команду «Открыть» в основном меню или на панели действий. При вызове команды открывается диалоговое окно, в котором пользователь указывает путь к каталогу с сохраненным Проектом паспорта ПО. Может быть использован файл с данными Проекта паспорта ПО или файл с данными Паспорта ПО в формате XML.

Если выполняется загрузка Проекта паспорта ПО и для данного клиента уже был сформирован Проект с более ранней датой формирования, то происходит замена на новый.

Если выполняется загрузка Проекта паспорта ПО с более ранней датой формирования, чем сохраненный для данного клиента Проект, выводится информационное сообщение, что выполняется загрузка Проекта с более ранней датой формирования, необходимо подтвердить замену Проекта паспорта ПО.

Проект паспорта ПО не может быть заверенным. Если подписать (заверить) Проект паспорта ПО, то он становиться Паспортом ПО.

Загрузка Паспорта ПО с СМН выполняется с помощью команды «Открыть» в основном меню или на панели действий. При загрузке Паспорта ПО автоматически выполняется контроль отсутствия модификации подписанного файла. Если Паспорт ПО прошел проверку, то он сохраняется как действующий Паспорт ПО.

Сохранение открытого Паспорта ПО либо Проекта паспорта ПО в формате XML (с расширением .pass) выполняется с помощью команды «Сохранить» в основном меню.

Загрузка нового заверенного Паспорта ПО с СМН выполняется с помощью команды «Применить». С помощью команды «Открыть» выполняется загрузка Паспорта ПО, после загрузки данных выполняется команда «Применить». При выполнении команды «Применить» осуществляется проверка:

- если дата формирования, дата утверждения, наименование импортируемого Паспорта ПО совпадает с датой формирования, датой утверждения, наименованием Паспорта ПО, который уже был сохранен на клиенте, выводится предупреждение, что такой Паспорт ПО существует с предложением заменить данную версию Паспорта ПО на импортируемую версию;
- если в Паспорте ПО наименование клиента не совпадает выводится сообщ0ение об отмене импорта Паспорта ПО.

После успешной проверки Паспорт ПО считается действующим.

Открытый Проект паспорта ПО можно сравнить с действующим Паспортом ПО и с любым другим Паспортом ПО. Команда «Паспорт» на панели «Сравнение» предназначена для автоматического

сравнения открытого Проекта паспорта ПО с действующим Паспортом ПО.

Результат сравнения отображается в рабочем поле формы, по результатам выполненного сравнения отображается список, который включает:

- данные по файлам в соответствии с таблицей 2;
- статус соответствия по каждому измененному файлу (новый, удален, изменен);
- наименование сравниваемых объектов (Проекта паспорта ПО, Паспорт ПО).

Команда «Файл» предназначена для выполнения сравнения открытого Паспорта ПО либо Проекта паспорта ПО с любым из сохраненных на ПК Паспортов ПО. После вызова команды открывается диалоговое окно, в котором пользователь указывает путь к каталогу с сохраненными Паспортами ПО. Результат сравнения отображается таким же образом, как описано выше.

Сохранение полученного сравнения формат RTF выполняется с помощью команды «Сохранить» в основном меню, а также с помощью команды «Сохранить как» в форматах RTF и TXT.

Если два Паспорта ПО содержат одинаковый список файлов с одинаковыми контрольными суммами, но порядок файлов в списках отличается, то данные Паспорта ПО будут считаться идентичными.

При выполнении сравнения автоматически выполняется контроль отсутствия модификации подписанного файла.

Удалить последний действующий Паспорт ПО или Проект паспорта ПО для ПК возможно с помощью команды «Удалить» на панели «Действия»:

- если открыт действующий Паспорт ПО для данного ПК, то выполняется удаление данного файла;
- если открыт Проект паспорта ПО для данного ПК, то выполняется удаление данного файла.

При централизованном режиме работы на клиенте всегда сохраняется только один действующий Паспорт ПО, который будет каждый раз перезаписываться (если был сформирован новый на СК).

Категория «Настойки» позволяет выполнять настройку и редактирование следующих параметров:

- Учетные данные:
  - имя компьютера;
  - тип компьютера;
  - наименование подразделения;
  - наименование автоматизированной системы;
  - рабочее место;
  - номер системного блока;
  - ответственный сотрудник;
  - начальник подразделения;
  - начальник подразделения ТЗИ;
  - начальник подразделения сопровождения.
- Параметры сканирования:
  - расписание сканирования;
  - исключить каталоги и файлы;
  - расширения сканируемых файлов.

В централизованном режиме управления настройки параметров сканирования наследуются от СК, выполняется наследование настроек расписания/периодичности сканирования, «Исключить каталоги и файлы», «Сканируемые файлы по расширениям». Учетные данные ПК настраиваются на ПК.

События подсистемы сканирования клиентской части фиксируются в журнале управления политиками. Фиксируются типы событий, приведенные в таблице 4.

Таблица 4. Фиксируемые типы событий для клиента

№	Тип события	Обязательные к регистрации данные	Момент добавления
1	Сканирование	• Идентификатор события (поле ID); • дата и время события (поле «Время»); • идентификатор компьютера (поле «Клиент»); • идентификатор пользователя (поле «Пользователь»); • результат (поле «Результат»): Успешно либо Ошибка (описание ошибки: этап, на котором выявлена ошибка; имя файла или	По завершению сканирования по команде пользователя (по команде «Построить») или в соответствии с установленным расписанием/периодом

№	Тип события	Обязательные к регистрации данные	Момент добавления
		каталога, при доступе к которому произошел сбой, или пустая строка, если произошла другая ошибка, не связанная с доступом; описание реакции на ошибку (сбор данных продолжается, сбор данных остановлен))	
2	Редактирование параметров	• Идентификатор события (поле ID); • дата и время события (поле «Время»); • идентификатор компьютера (поле «Клиент»); • идентификатор пользователя (поле «Пользователь»); • результат (поле «Результат»): Успешно либо Ошибка (описание ошибки)	После редактирования любого параметра сканирования
3	Загрузка Паспорта ПО со СМН	• Идентификатор события (поле ID); • дата и время события (поле «Время»); • идентификатор компьютера (поле «Клиент»); • идентификатор Паспорта ПО (поле «Дополнительно»); • идентификатор пользователя (поле «Пользователь»); • результат (поле «Результат»): Успешно либо Ошибка (описание ошибки)	После выполнения команды «Открыть» и выбора нужного файла из каталога
4	Синхронизация Паспортов ПО клиента	• Идентификатор события (поле ID); • дата и время события (поле «Время»); • идентификатор компьютера (поле «Клиент»); • идентификатор Паспорта ПО (поле «Дополнительно»); • идентификатор пользователя (поле «Пользователь»); • результат (поле «Результат»): Успешно либо Ошибка (описание ошибки)	После выполнения синхронизации между клиентом и сервером (в момент обращения клиента к серверу)

4.3 Создание учетных записей для автономного клиента

При установке СЗИ НСД необходимо дополнительно создавать группы Windows: Администратор ИБ, Администратор СК, Контролер, Аудитор.

В ОА на вкладке «Учетные записи» в раздел «Группы» необходимо добавить следующие группы (аналогично для СБ):

- Администратор ИБ;
- Администратор СК;
- Контролер, обладающий всеми полномочиями Аудитора, а также полномочиями на утверждение Паспорта ПО;
- Аудитор, обладающий полномочиями на просмотр Проектов паспортов ПО, Паспортов ПО, на выполнение сравнений.

Данные группы включают в себя привилегии в соответствии с таблицей 1.

При сохранении учетной записи необходимо выполнять проверку: учетной записи может быть назначена только одна группа СК.

4.4 Требования к лицензированию модуля «СК»

Если была введена лицензия без модуля «СК», то при вызове команды «Паспорт программного обеспечения» из раздела «Паспорт программного обеспечения» основного меню клиентской части DL, пользователю будет предложено сформировать отчет Паспорта ПО — ввести следующую информацию и сохранить файл отчета (Рис. 37):

- Учетные данные:
  - имя компьютера;

- тип компьютера;
- наименование подразделения;
- наименование автоматизированной системы;
- рабочее место;
- номер системного блока;
- ответственный сотрудник;
- начальник подразделения;
- начальник подразделения ТЗИ;
- начальник подразделения сопровождения.

- Параметры сканирования:
  - расписание сканирования;
  - исключить каталоги и файлы;
  - расширения сканируемых файлов.

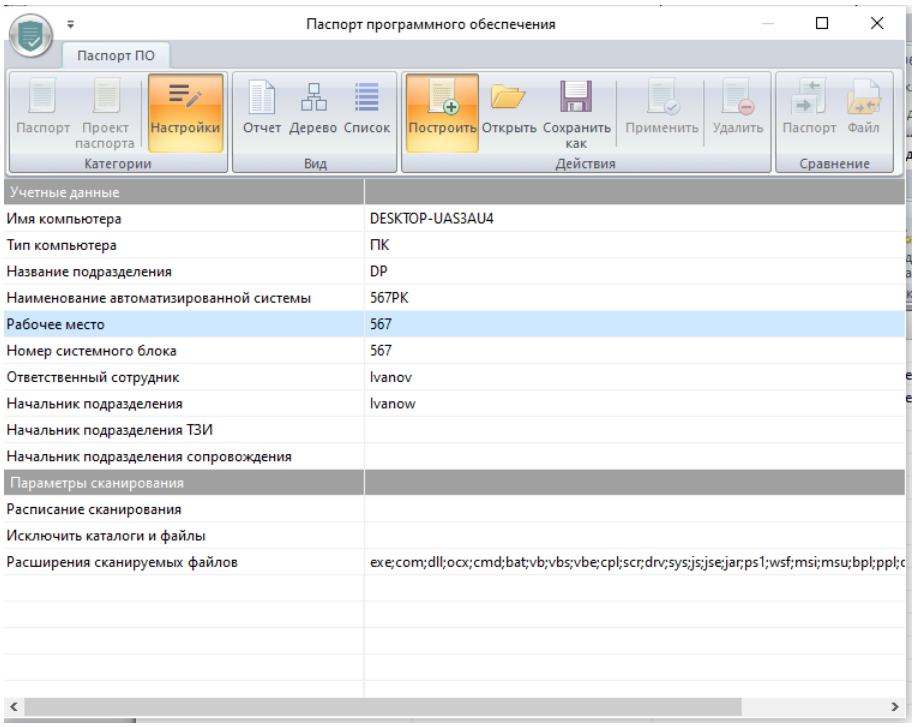


Рис. 37. Формирование отчета «Паспорт ПО»

Сохраненный отчет имеет вид, представленный на Рис. 38:

Паспорт программного обеспечения

Информация об отчете:	
Дата построения:	04.12.2020 12:49:35
Имя компьютера:	WIN-V580NJ7NNLE
Название подразделения:	konfi
Наименование АС:	WIN-N4QG043S
Рабочее место:	501
Операционная система:	Майкрософт Windows 8 Профессиональная 9200
Версия Dallas Lock:	СЗИ НСД Dallas Lock 8.0-C, сборка 689
Номер лицензии Dallas Lock:	
Максимальное кол-во терминальных сессий:	2
Номер системного блока:	344

Название ПО:	**Разработчик:**	**Назначение:**	**Объем (Кбайт):**	**Контрольная сумма:**	**Примечание:**
Greenshot 1.2.10.6	Greenshot		2966	354F16FA	
VMware Tools	VMware, Inc.		111752	BEC8BC8F	
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161	Microsoft Corporation		13532	B0EF8E24	
GoogleChrome	Google LLC			61F87A5D	
DallasLock8.0C	ООО "Конфидент"		503460	DB5FD4C7	
Dallas Lock 8.0. Сервер конфигураций	ООО "Конфидент"		7431	CDB356EB	
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161	Microsoft Corporation		10440	E2409D4B	
Dallas Lock 8.0. Сервер Безопасности. Демо-версия	ООО "Конфидент"		105148	EAC29730	

Начальник подразделения: Petrov P.
Подпись: _____
Начальник подразделения ТЗИ:
Подпись: _____
Начальник подразделения сопровождения:
Подпись: _____

Рис. 38. Отчет «Паспорт программного обеспечения»