



ТСС

Система контроля и разграничения доступа Diamond ACS

Инструкция по настройке и эксплуатации



Оглавление

1	Введение.....	4
2	Общие сведения о «Diamond ACS».....	5
3	Установка СКРД «Diamond ACS».....	7
3.1	Требования к аппаратному и программному обеспечению	7
3.2	Порядок установки	8
3.3	Установка «Diamond ACS AD Assistant»	8
3.4	Модифицирование схемы AD	12
3.5	Установка «Diamond ACS Security Server».....	13
3.5.1	Установка с СУБД «Microsoft SQL Server».....	13
3.5.2	Установка с СУБД «PostgreSQL»	21
3.6	Установка «Diamond ACS Security Manager» и «Security Monitor».....	22
3.7	Установка «Diamond ACS Agent Workstation Net».....	25
3.7.1	Установка на АРМ с ОС семейства Windows.....	25
3.7.2	Установка на АРМ с ОС семейства Linux.....	30
4	Активация «Diamond ACS».....	31
4.1	Регистрация в системе автоматической выдачи лицензий	32
4.2	Отправка запроса на получение лицензии	35
4.3	Получение запрошенных лицензий	39
4.4	Обновление лицензии СКРД «Diamond ACS».....	41
5	«Diamond ACS Security Manager».....	42
5.1	Основные принципы работы	42
5.2	Интерфейс.....	44
5.2.1	Главное окно программы.....	44
5.2.2	Главное меню	45
5.2.3	Панель инструментов.....	46
5.3	Управление лицензиями.....	47
5.3.1	Создание запроса.....	47
5.3.2	Импорт лицензий.....	51
5.3.3	Распределение лицензий.....	52
5.3.4	Удаление лицензий.....	52
5.4	Настройка сетевых параметров	53
5.4.1	Настройка порта сервера безопасности.....	53
5.4.2	Настройка интервала опроса Active Directory	55
6	«Diamond ACS Security Monitor».....	57
6.1	Запуск, идентификация и аутентификация	57
6.2	Панель инструментов	60
6.3	Окно мониторинга версий агентов.....	60
6.4	Контекстное меню действий над АРМ	62
6.5	Информационная панель.....	62
6.5.1	Просмотр общей информации.....	62
6.5.2	Контроль целостности данных.....	64
6.5.3	Просмотр журналов.....	66
6.6	Информация о сервере безопасности.....	67
6.6.1	Просмотр информации.....	67
6.6.2	Просмотр сессий.....	69
7	Типовые ошибки и способы их устранения	71
8	Глоссарий.....	74



Перечень сокращений

AD	Active Directory
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ЗИ	Защита информации
ИВС	Информационно-вычислительная система
ЛВС	Локальная вычислительная сеть
НЖМД	Накопитель на жестких магнитных дисках
НСД	Несанкционированный доступ
ПРД	Правила разграничения доступа
РСПД	Резервная система передачи данных
СВТ	Средство вычислительной техники
УС	Узел связи
САВЛ	Система автоматической выдачи лицензий
СУБД	Система управления базами данных



1 Введение

Данный документ предназначен для администратора системы контроля и разграничения доступа «**Diamond ACS**» и охватывает процесс установки, первоначальной настройки. Подробное руководство по настройке и эксплуатации системы контроля и разграничения доступа «Diamond ACS» изложено в документе «Система контроля и разграничения доступа Diamond ACS. Руководство администратора 91 5051-001-61649217-10», документ доступен в разделе «Документация», подразделе «ACS» по адресу <ftp://office.tssltd.ru>.

Сайт в Интернете. Если у вас есть доступ в Интернет, вы можете посетить сайт компании ООО «ТСС» (<http://tssltd.ru/>) или связаться с представителями компании по электронной почте (support@tssltd.ru).

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8-(800) 500-43-68 или по электронной почте support@tssltd.ru

Учебные курсы. Освоить аппаратные и программные продукты компании ТСС можно на курсах Учебного центра. Связаться с представителем Учебного центра можно по электронной почте (sales@tssltd.ru).



2 Общие сведения о «Diamond ACS»

Функциональные возможности системы контроля и разграничения доступа позволяют применять ее для обеспечения защиты от НСД к информации на автономных компьютерах и рабочих станциях ЛВС (типа IBM PC AT), функционирующих под управлением:

- Windows 8/8.1;
- Windows 7;
- Windows Vista;
- Windows XP;
- Windows Server 2012 /2012 R2;
- Windows Server 2008/2008 R2;
- Red Hat Enterprise Linux 6;
- Windows 10;
- Linux 2.6 kernel;
- Linux 3.x kernel;
- DmOS

В системах терминального доступа, построенных на базе терминальных служб сетевых ОС Windows и программного обеспечения Citrix (MetaFrame и др. функционирующего на базе протокола ICA), а также в АС, построенных на их основе, в многопользовательском режиме эксплуатации.

СКРД «Diamond ACS» обеспечивает выполнение требований ТУ 5015-001-61649217-10, а также руководящих документов «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) - по 3 классу защищенности и «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» (Гостехкомиссия России, 1999) - по 2 уровню контроля, что дает возможность использования комплекса в АС в соответствии с п. 2.18 руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992) до класса 1Б включительно и для защиты информации в информационных системах персональных данных до 1 класса включительно.



Структурно комплекс состоит из взаимосвязанных подсистем:

- системы управления безопасностью, мониторинга и аудита, включающей в себя программные модули «Diamond ACS AD Assistant», «Diamond ACS Security Server», «Diamond ACS Security Manager», «Diamond ACS Security Monitor».
- системных агентов, включающих в себя программный модуль «Diamond ACS Agent Workstation Net», аппаратный модуль «Diamond ACS Agent HW» и идентификатор пользователя «Diamond ACS Key/Diamond ACS Key Lt».

Комплекс обеспечивает возможность совместной работы с со следующими СЗИ и СКЗИ:

- по части обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений – Diamond VPN/FW (производства ООО «ТСС», сертификат соответствия ФСТЭК России №2260 от 21 января 2011 г.), Dcrypt 1.0 (производства ОАО «БИТК», сертификаты соответствия ФСБ России № СФ/124-2701, СФ/124-2702, СФ/124-2703 от 25 августа 2015 г.)
- для хранения ключевой и идентифицирующей информации – JaCart (производства ООО «АЛАДДИН-РД», сертификат ФСТЭК России №3449 от 7 сентября 2016 г.), RuToken (производства ООО «АКТИВ», сертификат ФСТЭК России №2584 от 12 марта 2012 г.).



3 Установка СКРД «Diamond ACS»

Установка СКРД «Diamond ACS» возможна двумя способами:

- автоматическая установка средствами Active Directory (только для ОС семейства Windows);
- ручная установка.

В режиме автоматической установки средствами Active Directory администратор безопасности получает возможность установки подсистем СКРД одновременно на несколько АРМ. По причине применения средств Active Directory, использование данного способа установки возможно только для АРМ с установленной ОС семейства Windows.

В режиме ручной установки инсталляция подсистем СКРД «Diamond ACS» производится последовательно на каждом АРМ.

3.1 Требования к аппаратному и программному обеспечению

Системные ограничения: рекомендуется устанавливать СКРД «Diamond ACS» до установки антивирусов, DLP-систем и межсетевых экранов, либо отключив их на время установки СКРД «Diamond ACS».

Требования к доменной инфраструктуре

Поддерживаемые ОС контроллера домена:

- Windows Server 2003 SP2/Server 2003 R2 SP2;
- Windows Server 2008 SP2/Server 2008 R2 SP1;
- Windows Server 2012 /Server 2012 R2.

Ограничений на количество рабочих станций, управляемых одним сервером Diamond ACS, нет. Максимальное количество АРМ определяется ресурсами сервера (оперативной памятью, процессором, дисковой подсистемой и т.д.).

Предварительно все рабочие станции и пользователи должны быть зарегистрированы в домене. На всех АРМ должны быть созданы профайлы для всех требуемых пользователей, установлено требуемое аппаратное и программное обеспечение, и проверена его работоспособность (в т. ч. работоспособность специализированных устройств: плоттеров, считывателей смарт-карт, аппаратных ключей, плат PCI/PCI Express, HASP ключей и др.).



3.2 Порядок установки

Перед началом установки и настройки СКРД «Diamond ACS» необходимо ознакомиться с общими сведениями о «Diamond ACS» (см. раздел 2) и требованиями к аппаратному и программному обеспечению (см. п. 3.1).

Рекомендуемый порядок установки и настройки СКРД «Diamond ACS»:

1. Установить утилиту «Diamond ACS AD Assistant» (см. п.3.3).
2. Модифицировать схему Active Directory, используя утилиту «Diamond ACS AD Assistant» (см. п. 3.4).
3. Установить приложение «Diamond ACS Security Server» (см. п. 3.5).
4. Установить компоненты «Diamond ACS Security Manager» и «Diamond ACS Security Monitor» (см. п. 3.6).
5. Создать файл запроса лицензий, используя приложение «Diamond ACS Security Manager» (см. п. 5.3.1).
6. Получить файл с лицензиями, используя WEB-сервис для автоматизированного получения лицензий (см. п. 4.3).
7. Использовать полученный файл с лицензиями (см. п. 5.3.2).
8. При наличии аппаратного модуля «Diamond ACS HW» произвести его установку.
9. Установить приложение «Diamond ACS Agent Workstation Net» (см. п. 3.7).

3.3 Установка «Diamond ACS AD Assistant»

Для установки приложения «Diamond ACS AD Assistant» необходимо:

1. Запустить файл DmADAssistant.msi.
2. В появившемся окне нажать кнопку «Далее» (см. рисунок 1).

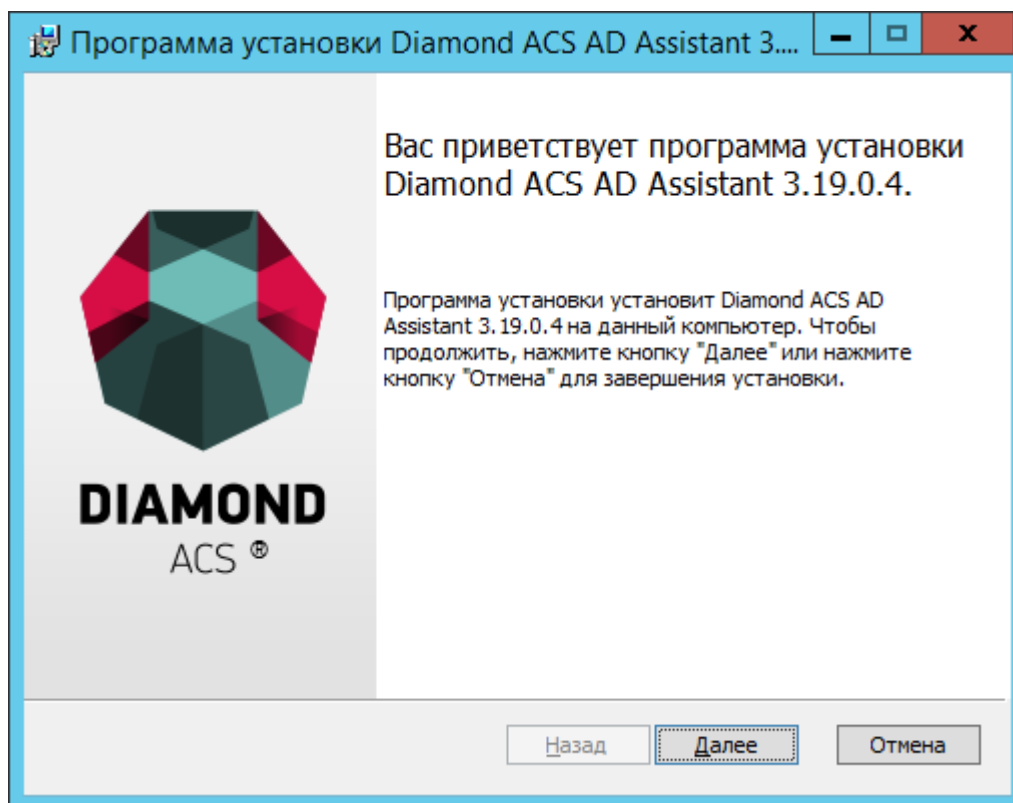


Рисунок 1 – Окно приветствия программы установки

3. Ознакомиться с лицензионным соглашением.
4. В случае принятия условий лицензионного соглашения, поставить отметку рядом с полем «Я принимаю условия лицензионного соглашения» (см. рисунок 2).
5. Нажать кнопку «Далее».

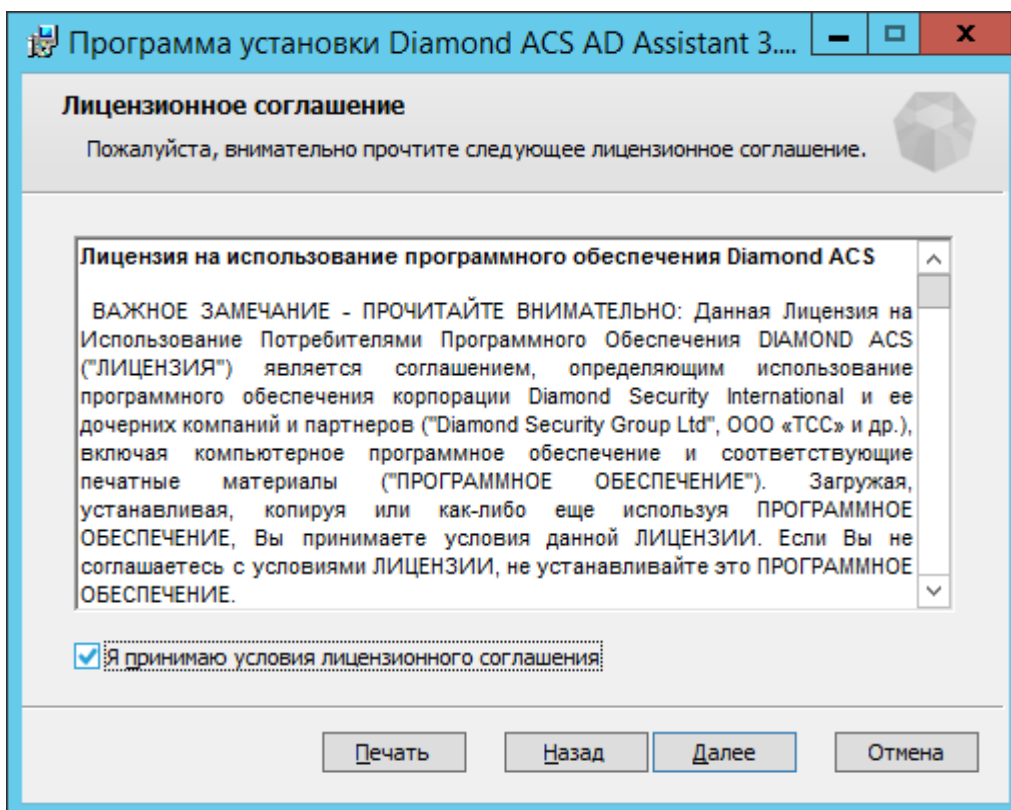


Рисунок 2 – Окно принятия условий лицензионного соглашения

6. Выбрать путь для установки приложения или оставить путь, предлагаемый по умолчанию (см. рисунок 3).
7. Нажать кнопку «Далее».

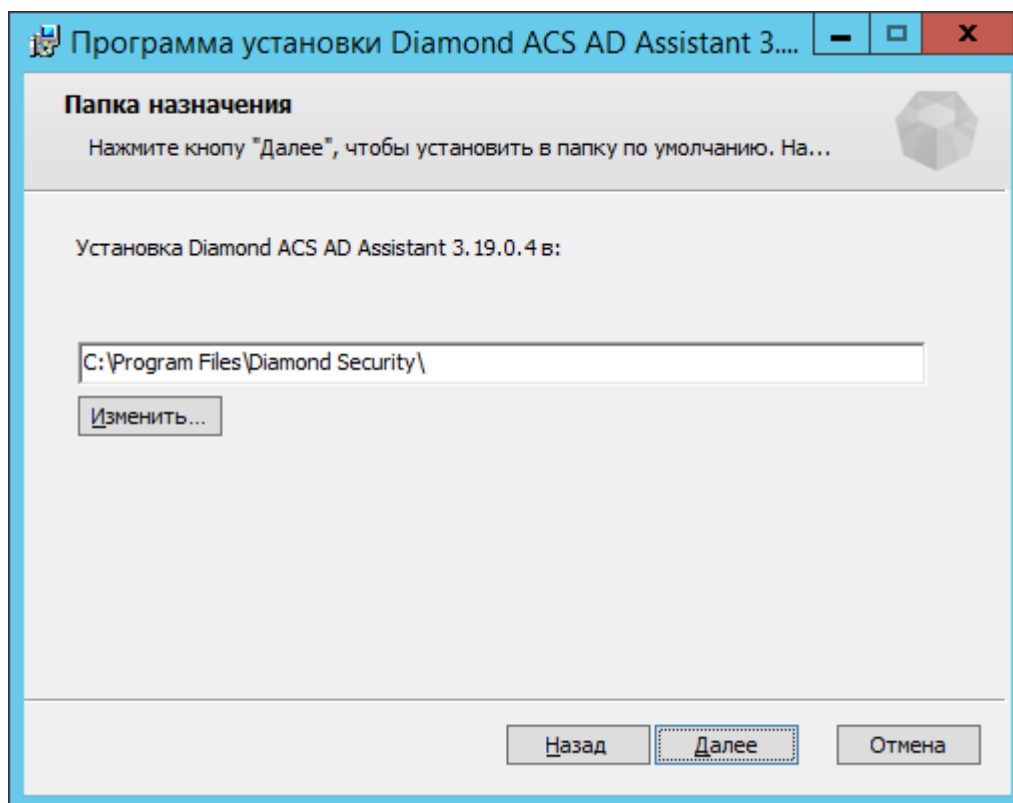


Рисунок 3 – Выбор пути установки

8. Нажать кнопку «Установить» (см. рисунок 4).

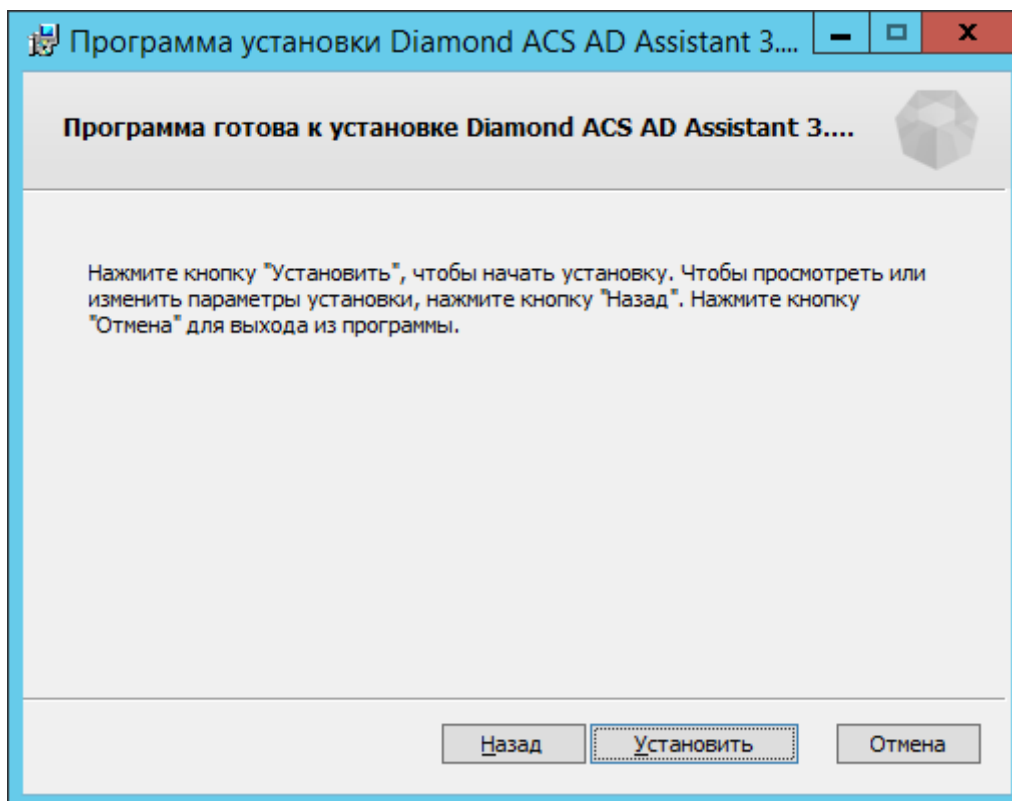


Рисунок 4 – Положение кнопки установить



9. Дождаться окончания установки и нажать кнопку «Готово» (см. рисунок 5).

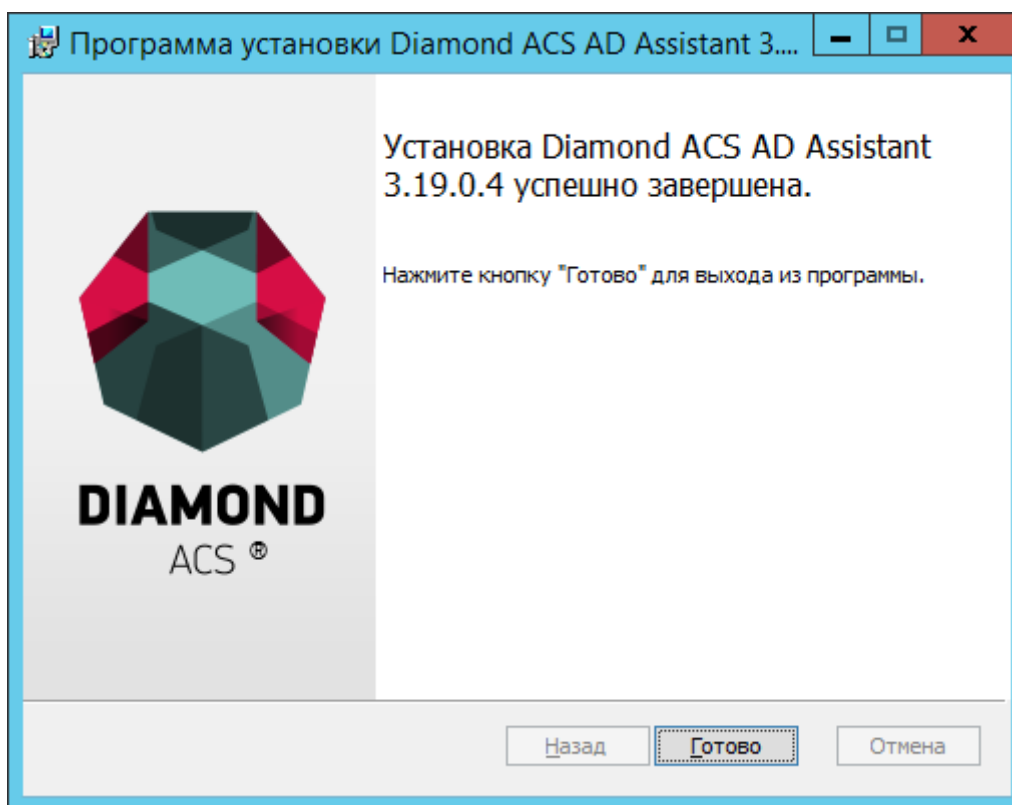


Рисунок 5 – Положение кнопки готово

3.4 Модифицирование схемы AD

Внимание! Перед модификацией схемы необходимо убедиться, что контроллер домена, выполняющий FSMO роль «Хозяин схемы» («Schema master») доступен по сети. Для этого выполнить команду `netdom query fsmo`. В случае двух контроллеров домена данные между ними должны быть реплицированы.

Для модифицирования схемы Active Directory необходимо:

1. Запустить приложение «Diamond ACS AD Assistant»;
2. Ввести в поле «Контроллер домена» доменное имя контроллера домена;
3. Ввести в поля «Логин» и «Пароль» соответственно логин и пароль учетной записи пользователя, являющегося членом групп «Администраторы схемы» и «Администраторы домена»;
4. Нажать кнопку «Обновить схему AD».



3.5 Установка «Diamond ACS Security Server»

Сервер безопасности «Diamond ACS» требует наличия установленной и настроенной СУБД «Microsoft SQL Server» 2008/2012/2014 или «PostgreSQL» 9.x. В случае использования «Microsoft SQL Server» необходим именованный экземпляр СУБД, использующий для соединений режим проверки подлинности Windows или смешанный режим. Для установки «Diamond ACS Security Server» с «PostgreSQL» в СУБД должен быть настроен метод аутентификации SSPI, и создана роль входа «система» («SYSTEM» – для англоязычной ОС), обладающая всеми привилегиями (установлены флаги для ролей public и sysadmin).

3.5.1 Установка с СУБД «Microsoft SQL Server»

Для установки приложения «Diamond ACS Security Server» с СУБД «Microsoft SQL Server» необходимо:

1. Запустить файл DmServer.msi. Для расследования проблем в случае неуспешной установки желательно установку делать с логированием, т.е. запустить файл инсталлятора через командную строку. Перейти в командной строке в директорию, где расположен файл DmServer.msi и выполнить команду:
 - `msiexec /i DmServer.msi /log DmServer_installation_log.txt`
2. В появившемся окне нажать кнопку «Далее» (см. рисунок 6).

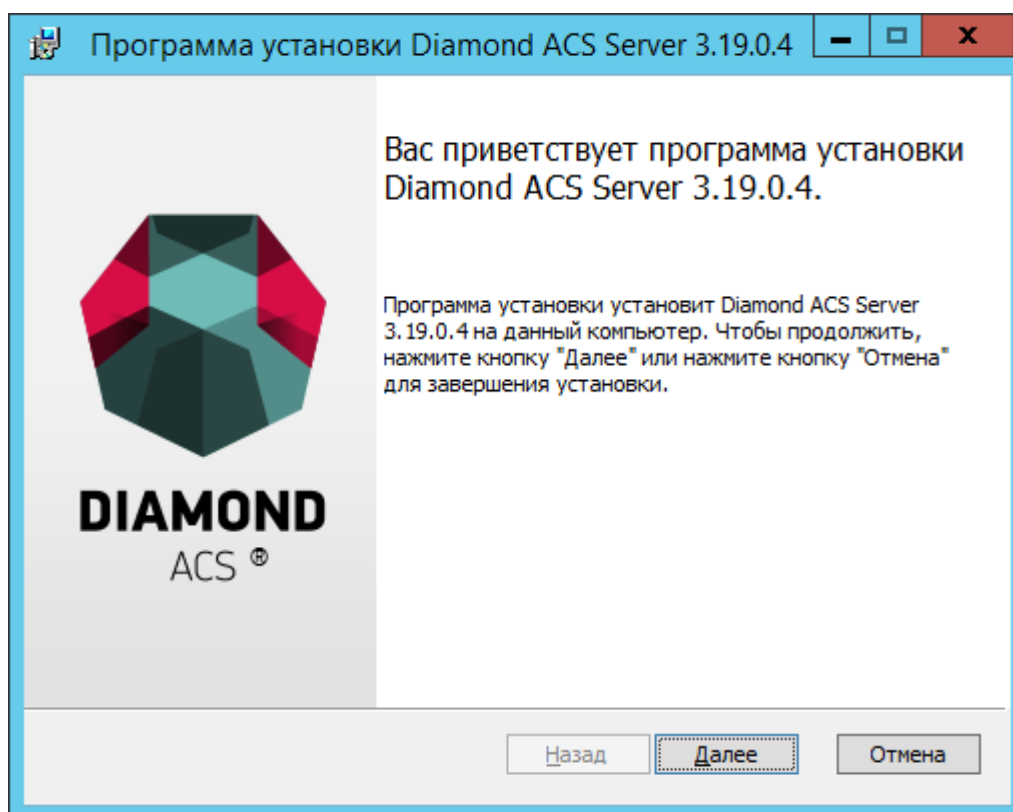


Рисунок 6 – Положение кнопки «Далее»

3. Ознакомиться с лицензионным соглашением.
4. В случае принятия условий лицензионного соглашения, поставить отметку рядом с полем «Я принимаю условия лицензионного соглашения» и нажать кнопку «Далее» (см. рисунок 7).

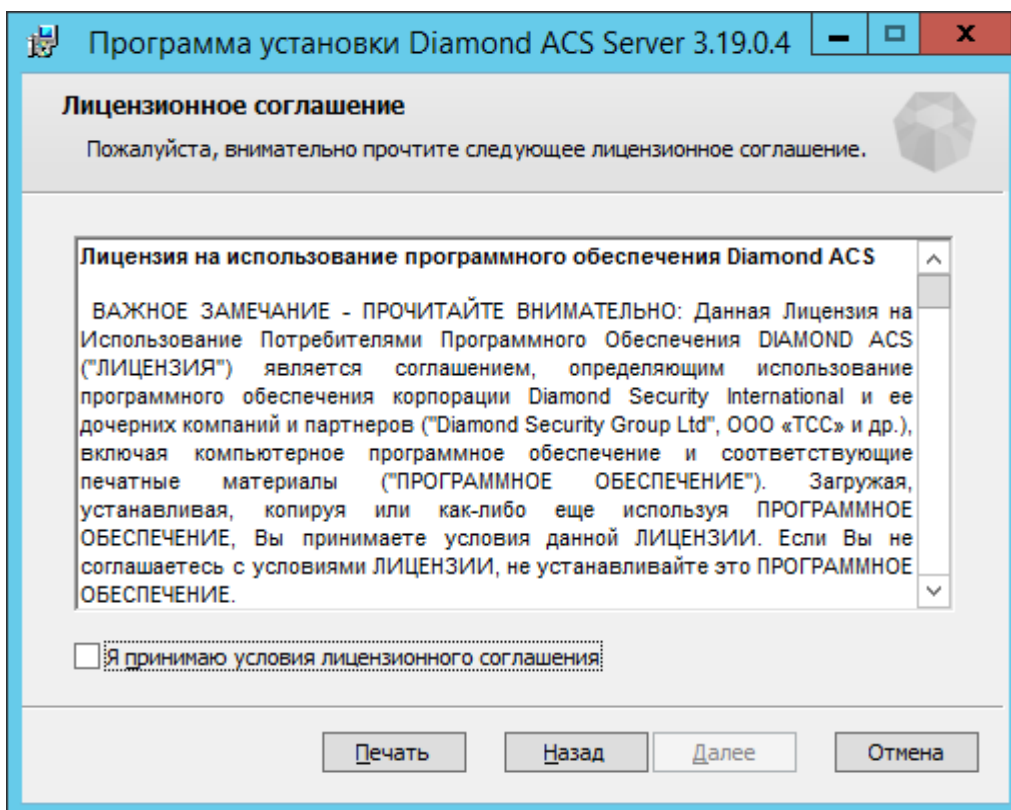


Рисунок 7 – Окно принятия условий лицензионного соглашения

5. Выбрать путь для установки приложения или оставить путь, предлагаемый по умолчанию и нажать кнопку «Далее» (см. рисунок 8).

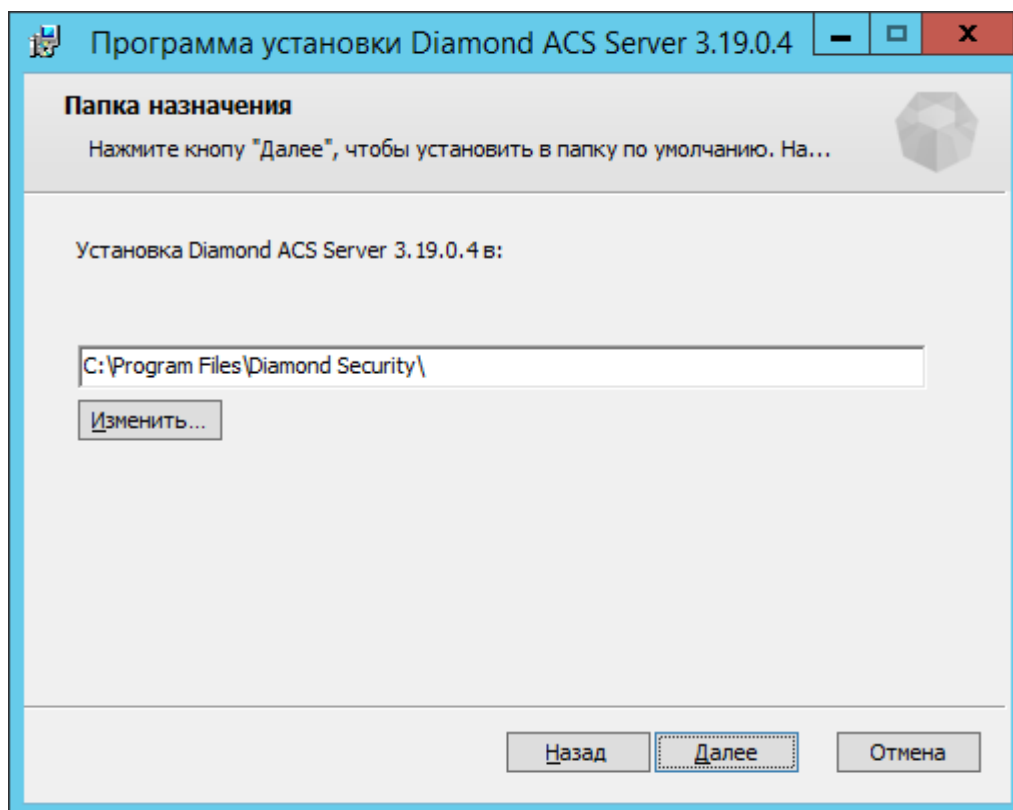


Рисунок 8 – Выбор пути установки

6. Ввести логин и пароль администратора домена и нажать кнопку «Далее» (см. рисунок 9).

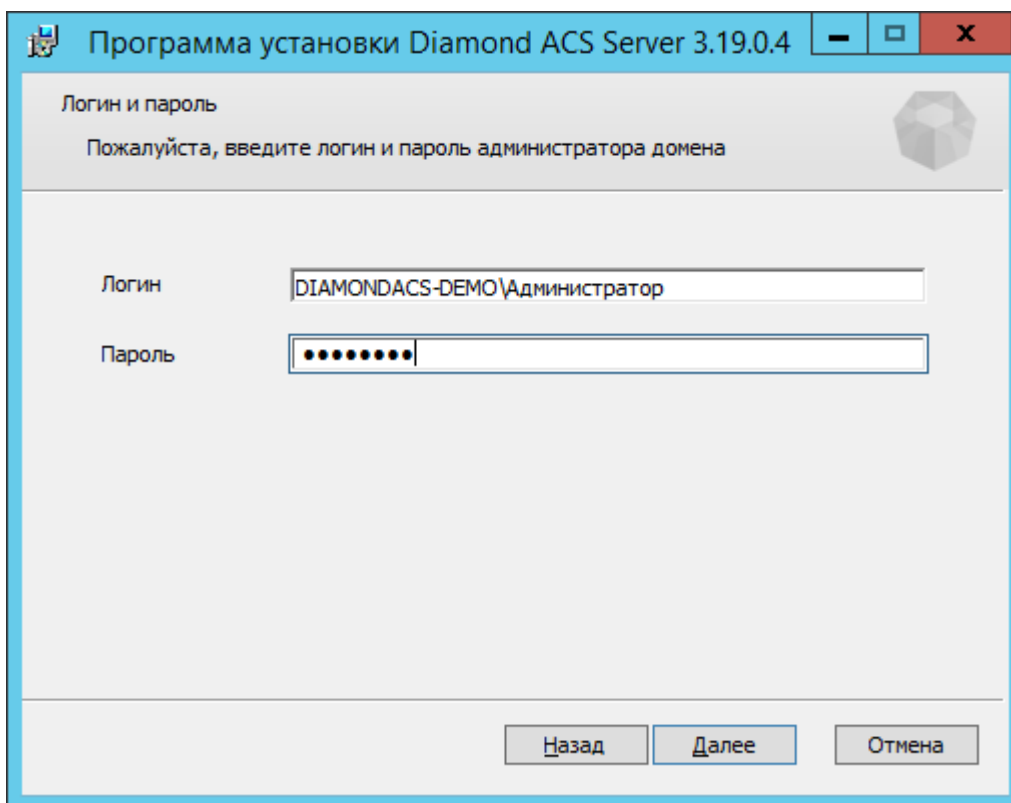


Рисунок 9 – Окно ввода «Логин», «Пароль» Администратора домена

7. Ввести имя базы данных или оставить имя, предложенное по умолчанию.
8. Выбрать тип SQL сервера: «MS SQL» (см. рисунок 10).

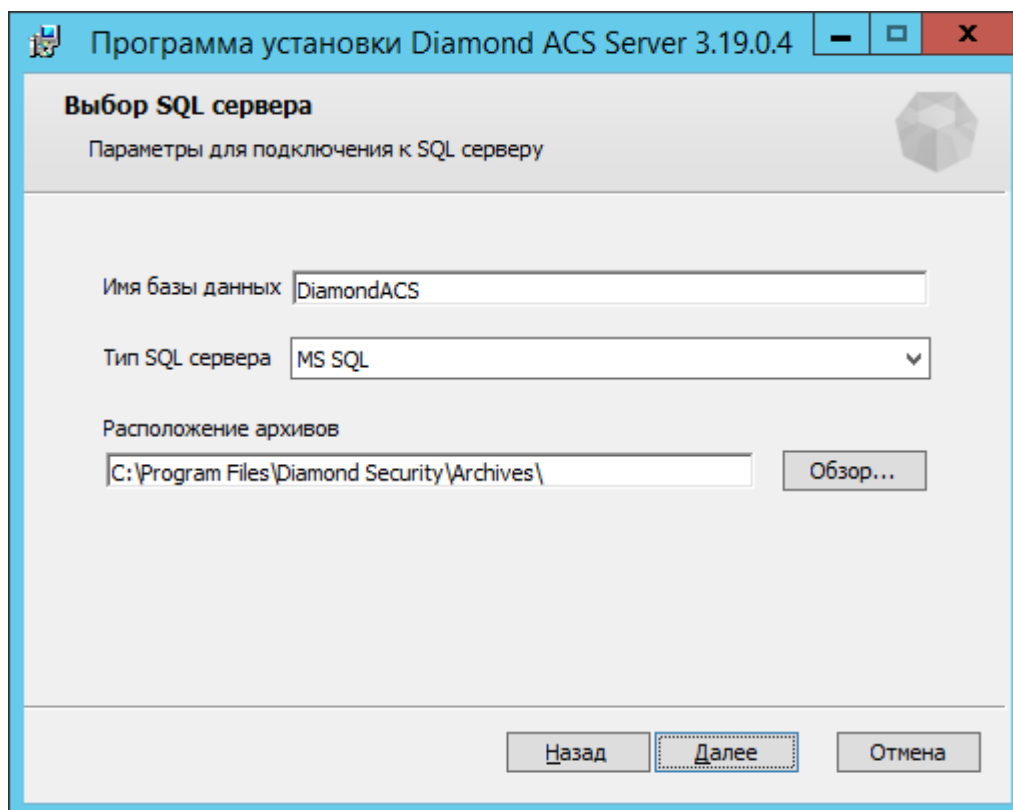


Рисунок 10 – Окно выбора SQL сервера

9. Если на момент установки в экземпляре СУБД имеется база данных с указанным именем, то процесс установки «Diamond ACS Security Server» будет завершен с ошибкой и существующая база не будет удалена. Необходимо заново запустить процесс установки и задать другое имя базы данных, которое не используется на данном экземпляре SQL Server.
10. Нажать кнопку «Далее».
11. Ввести имя экземпляра СУБД «Microsoft SQL Server» (см. рисунок 11). Имя экземпляра имеет формат: А\Э, где А – имя или IP-адрес компьютера; Э – имя экземпляра SQL Server. Если экземпляр СУБД установлен в той же системе, в которой производится установка сервера безопасности, то в качестве имени компьютера возможно использование «localhost» или символа «.».

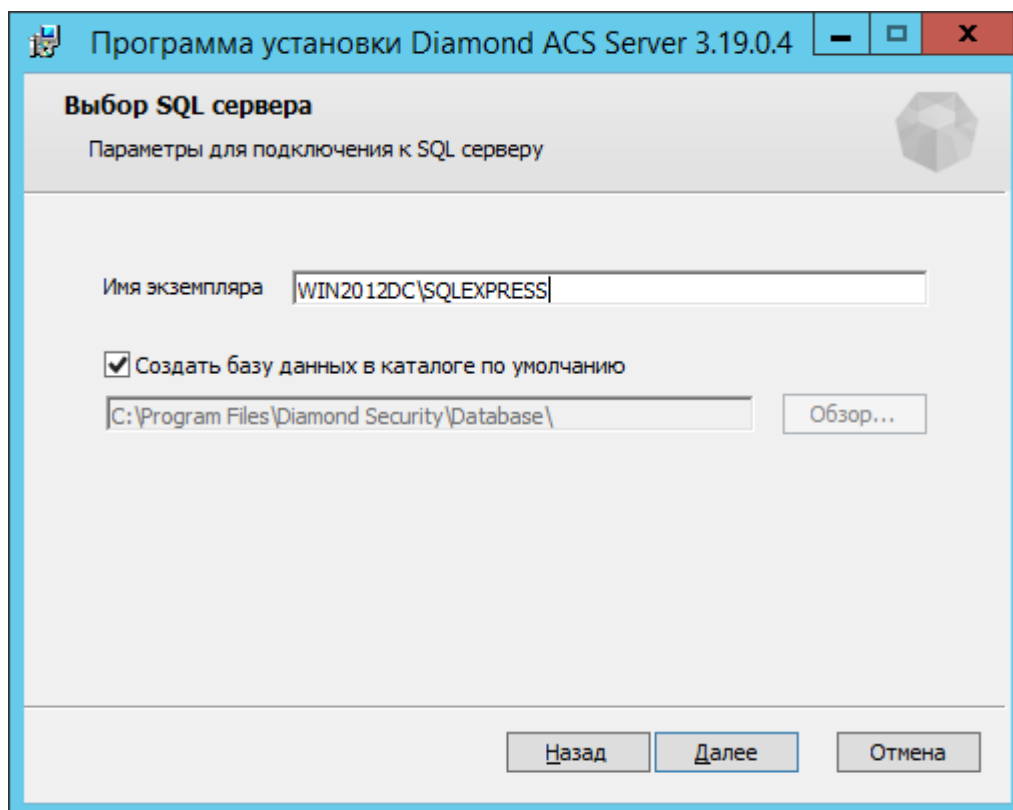


Рисунок 11 – Окно ввода имени экземпляра СУБД «Microsoft SQL Server»

12. Оставить отметку рядом с полем «Создать базу данных в каталоге по умолчанию» или, сняв отметку, указать каталог, в котором будут созданы файлы базы данных и нажать кнопку «Далее».
13. Нажать кнопку «Установить» (см. рисунок 12).

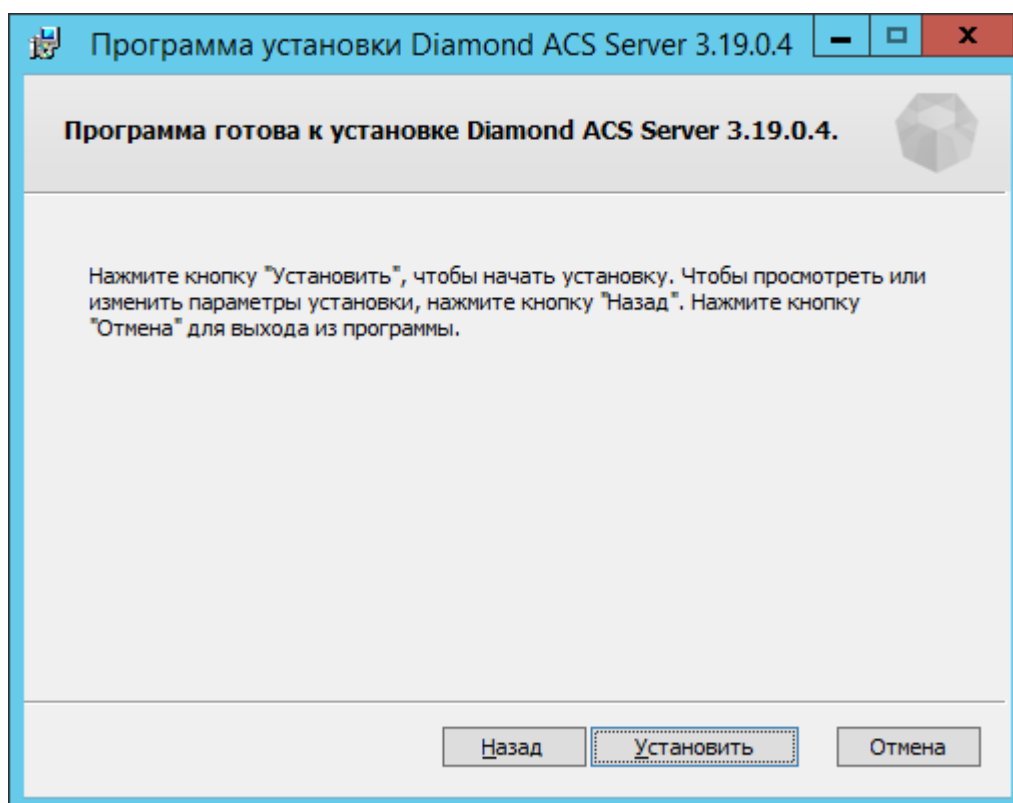


Рисунок 12 – Положение кнопки «Установить»

14. Дождаться окончания установки и нажать кнопку «Готово».

Для случая, если сервер баз данных «Microsoft SQL Server» и сервер безопасности «Diamond ACS Server» установлены на разных компьютерах необходимо выполнить следующие настройки:

1. Запустить SQL Server Configuration Manager.
2. Выбрать пункт «Сетевая конфигурация SQL Server», «Протоколы для <имя_именованного_экземпляра>».
3. Для «TCP/IP» выбрать пункт контекстного меню «Свойства».
4. На вкладке «Протокол» установить «Включено» = «Да».
5. На вкладке «IP-адреса» в разделе «IPAll» задать значение TCP-порта.
6. Перезапустить SQL Server.
7. В межсетевом экране создать правило для этого TCP-порта, разрешающее входящие соединения.
8. В межсетевом экране создать правило для UDP-порта 1434 для SQL Server Обозреватель, разрешающее входящие соединения.
9. С помощью «Microsoft SQL Server Management Studio» подключиться к серверу баз



данных, куда будет произведена установка базы данных сервера безопасности «Diamond ACS Server».

10. В иерархии обозревателя объектов выбрать пункт «Безопасность -> Имена входа».
11. В контекстном меню выбрать пункт «Создать имя входа...».
12. На странице «Общие» в поле «Имя входа» ввести имя компьютера, на который установлен сервер безопасности «Diamond ACS Server в формате <имя_домена\имя_компьютера\$>».
13. На странице «Роли сервера» установить флаг «sysadmin» и нажать «ОК».

3.5.2 Установка с СУБД «PostgreSQL»

Для установки приложения «Diamond ACS Security Server» с СУБД «Microsoft SQL Server» необходимо:

1. Запустить файл DmServer.msi.
2. В появившемся окне нажать кнопку «Далее».
3. Ознакомиться с лицензионным соглашением.
4. В случае принятия условий лицензионного соглашения, поставить отметку рядом с полем «Я принимаю условия лицензионного соглашения» и нажать кнопку «Далее».
5. Выбрать путь для установки приложения или оставить путь, предлагаемый по умолчанию, и нажать кнопку «Далее».
6. Ввести логин и пароль администратора домена и нажать кнопку «Далее».
7. Ввести имя базы данных или оставить имя, предложенное по умолчанию.
8. Выбрать тип SQL сервера: «PostgreSQL».
9. Если на момент установки в экземпляре СУБД имеется база данных с указанным именем, то в процессе установки «Diamond ACS Security Server» существующая база будет удалена. Чтобы избежать потери данных, хранящихся в существующей базе, необходимо оставить отметку рядом с полем «Сделать резервную копию существующей базы» и выбрать путь для файла резервной копии.
10. Нажать кнопку «Далее».
11. Ввести имя или IP-адрес компьютера и порт установленной СУБД «PostgreSQL» и нажать кнопку «Далее».
12. Нажать кнопку «Установить».
13. Дождаться окончания установки и нажать кнопку «Готово».



3.6 Установка «Diamond ACS Security Manager» и «Security Monitor»

Для установки приложений «Diamond ACS Security Manager» и «Diamond ACS Security Monitor» необходимо:

1. Запустить файл DmMonitor.msi (см. рисунок 13).

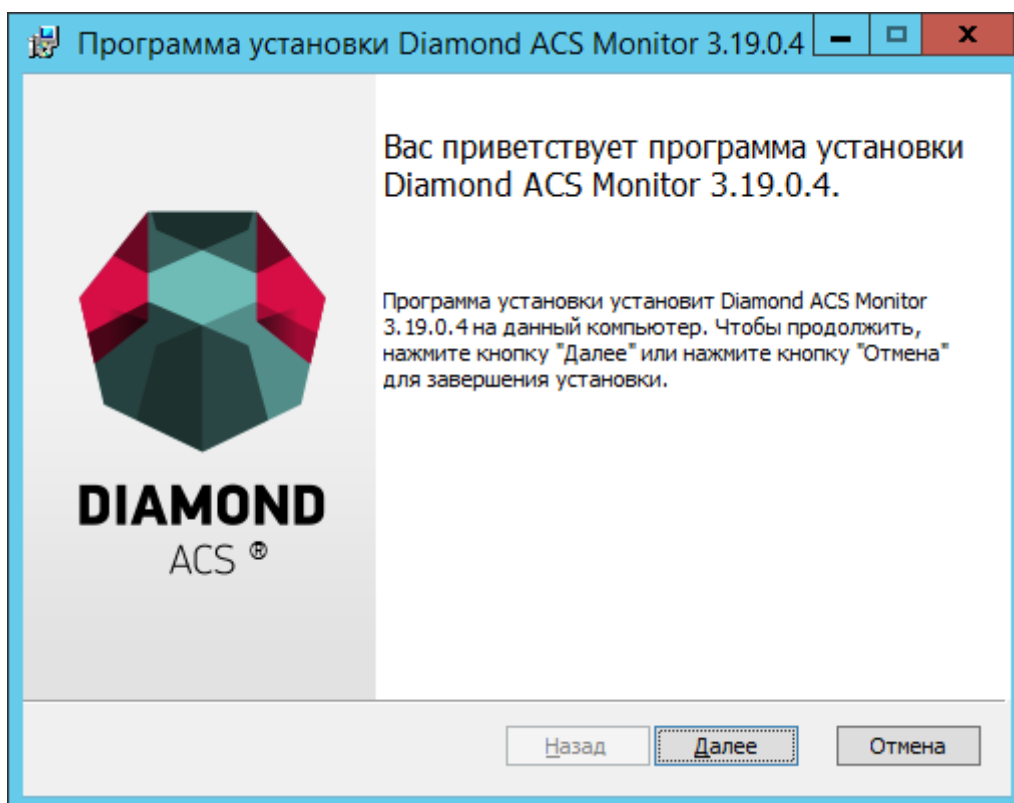


Рисунок 13 – Окно установки «Diamond ACS Monitor»

2. В появившемся окне нажать кнопку «Далее».
3. Ознакомиться с лицензионным соглашением (см. рисунок 14).

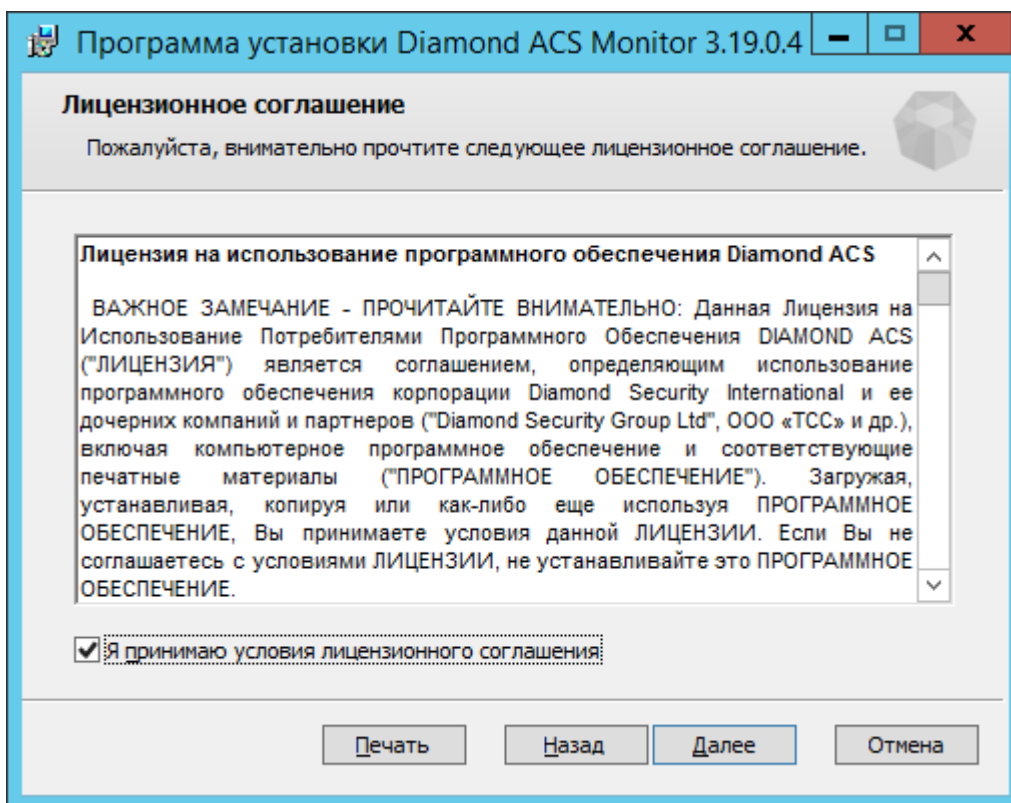


Рисунок 14 – Окно принятия условий лицензионного соглашения

4. В случае принятия условий лицензионного соглашения, поставить отметку рядом с полем «Я принимаю условия лицензионного соглашения» и нажать кнопку «Далее».
5. Выбрать путь для установки приложения или оставить путь, предлагаемый по умолчанию, и нажать кнопку «Далее» (см. рисунок 15).

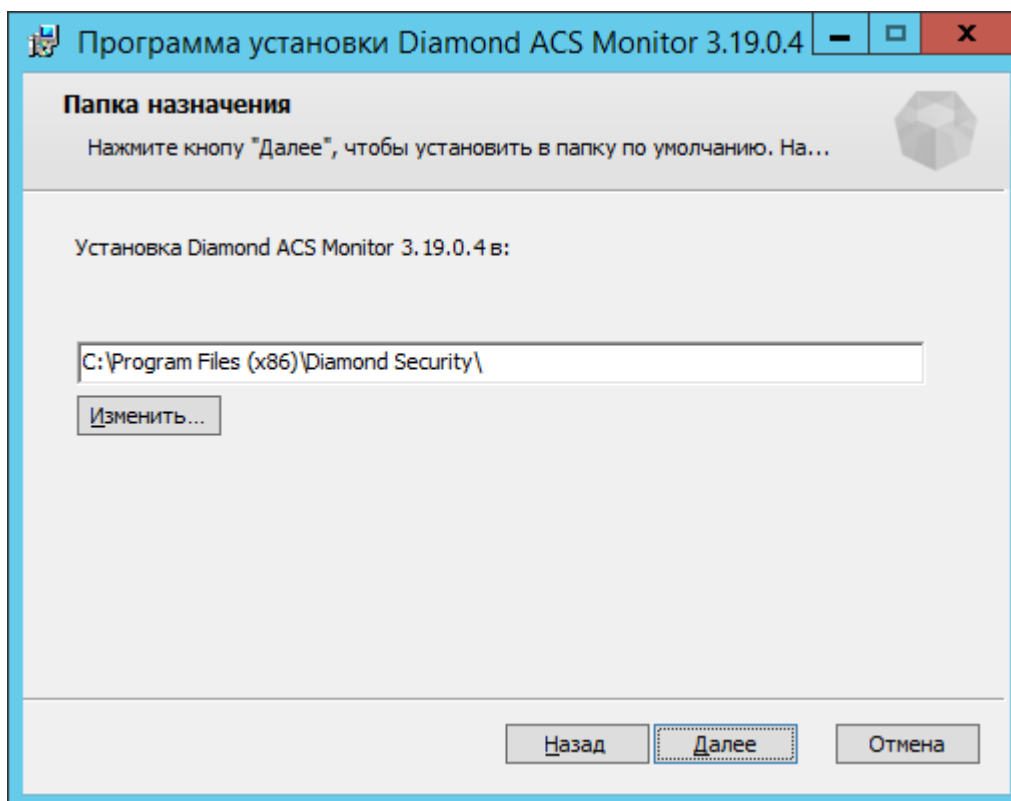


Рисунок 15 – Окно выбора пути установки

6. Нажать кнопку «Установить» (см. рисунок 16).

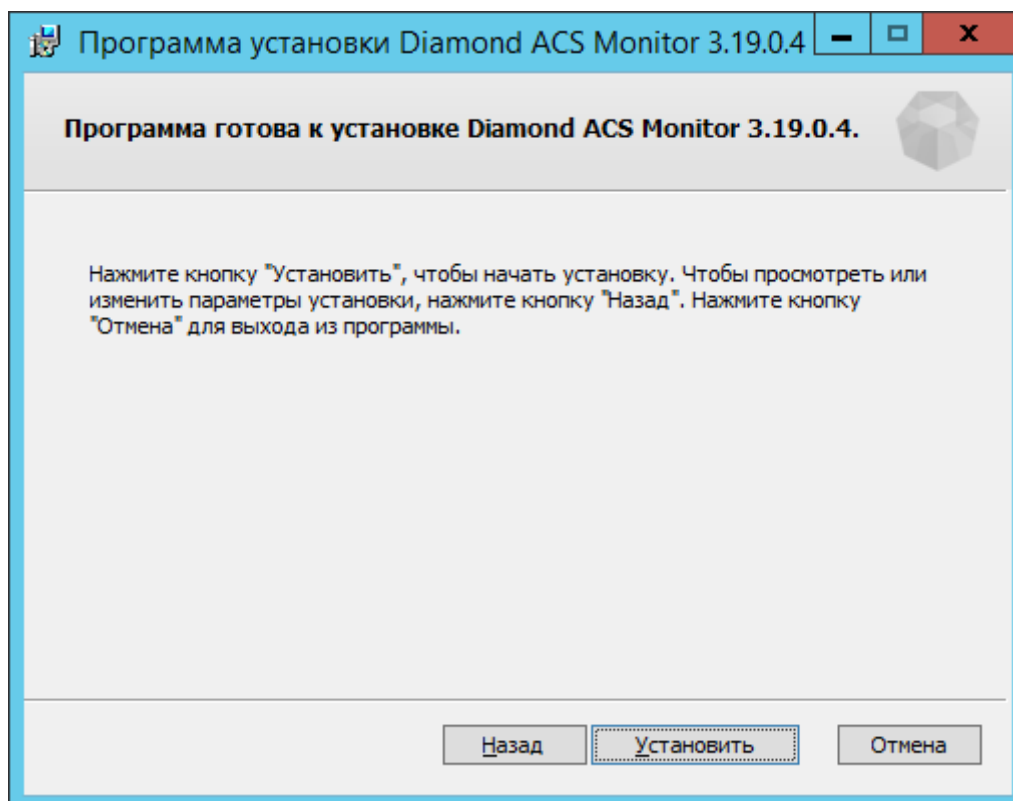


Рисунок 16 – Положение кнопки «Установить»



7. Дождаться окончания установки и нажать кнопку «Готово» (см. рисунок 17).

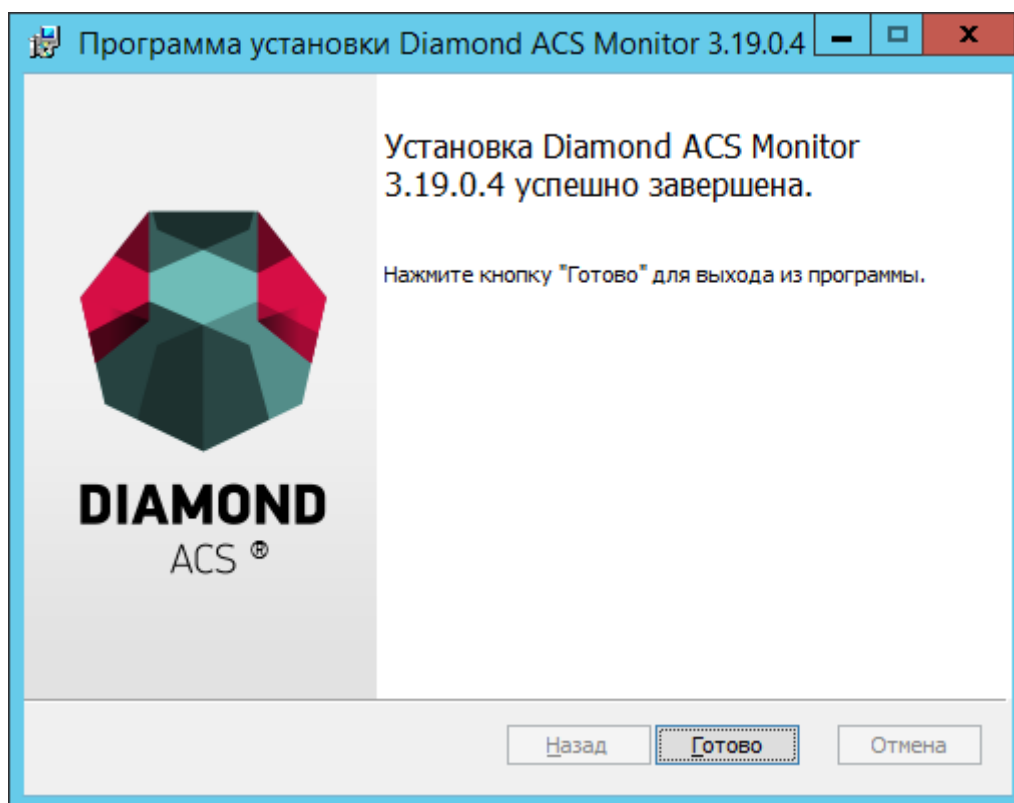


Рисунок 17 – Положение кнопки «Готово»

3.7 Установка «Diamond ACS Agent Workstation Net»

3.7.1 Установка на APM с ОС семейства Windows

Внимание! До установки должны быть уже импортированы лицензии для агентов. В момент установки должен быть доступен контроллер домена, на котором хранятся установленные лицензии для компонентов «Diamond ACS».

3.7.1.1 Установка средствами Active Directory

Для установки приложения «Diamond ACS Agent Workstation Net» средствами оснастки Active Directory «Пользователи и компьютеры» необходимо:

1. Создать два подразделения (organizational unit или OU): для x86 и x64 APM.
2. Поместить защищаемые APM в соответствующие подразделения в зависимости от разрядности установленной операционной системы.
3. Желательно для расследования причин ошибок при установке агента включить запись в лог событий установщика Windows через оснастку Windows «Управление групповой



политикой». Для этого изменить объект «Default Domain Policy». В «Редактор» управления групповыми политиками для установщика Windows включить политики «Задать типы событий, записываемых установщиком Windows в журнал транзакций» и задать значение iwear.

4. Назначить созданным подразделениям новые групповые политики, задав событие установки СКРД «Diamond ACS» на клиентские рабочие места.

Установка «Diamond ACS Agent Workstation Net» произойдет в тот момент, когда ОС на клиентском АРМ произведет обновление параметров групповых политик Active Directory.

3.7.1.2 Ручная установка

Для ручной установки программного модуля «Diamond ACS Agent Workstation Net» необходимо:

1. Запустить файл DmAgent.msi
2. В появившемся окне нажать кнопку «Далее» (см. рисунок 18).

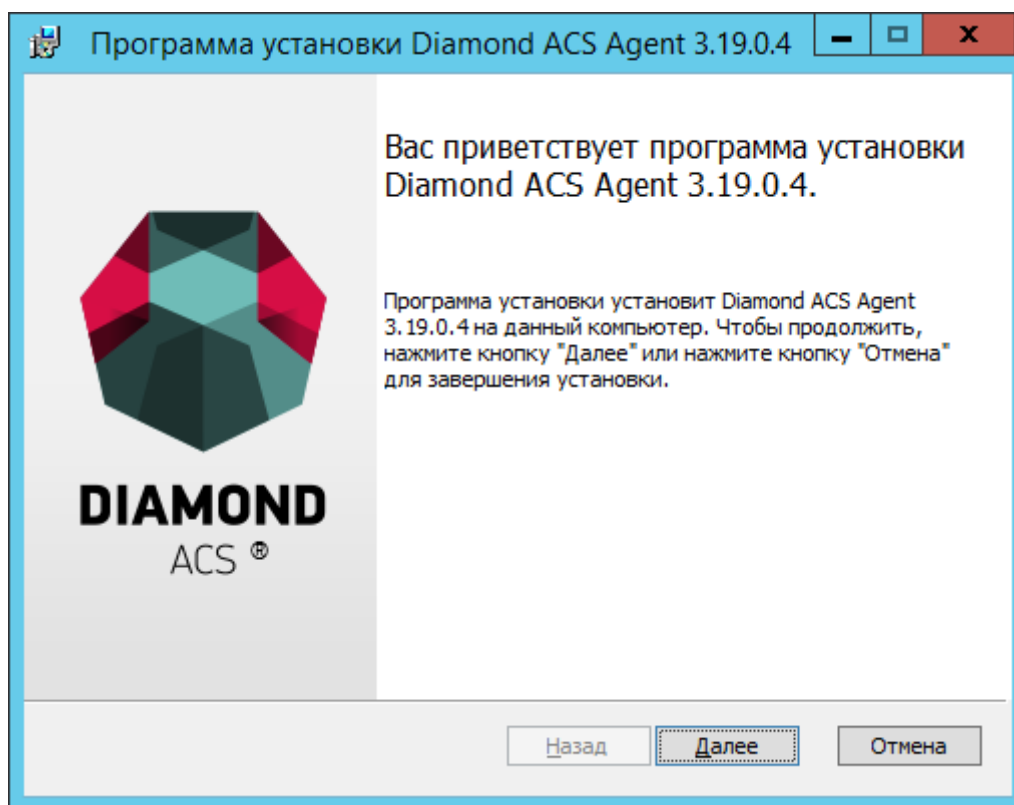


Рисунок 18 – Окно установки «Diamond ACS Agent»

3. Ознакомиться с лицензионным соглашением.
4. В случае принятия условий лицензионного соглашения, поставить отметку рядом с



полю «Я принимаю условия лицензионного соглашения» и нажать кнопку «Далее» (см. Рисунок 19).

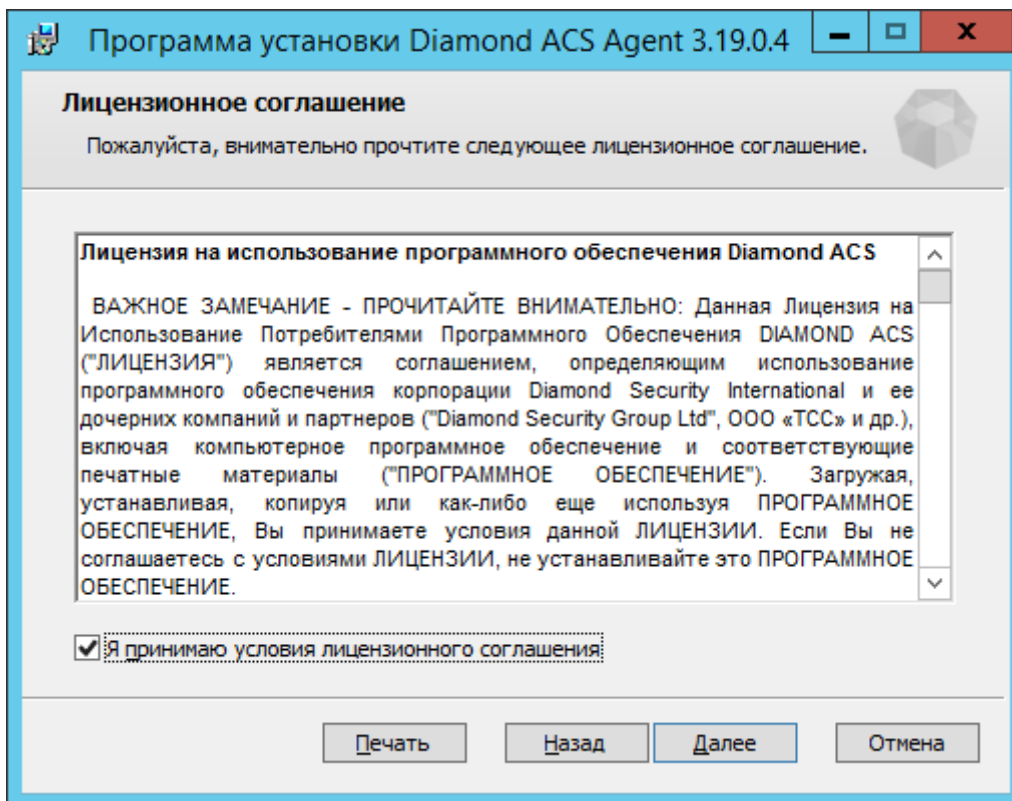


Рисунок 19 – Окно принятия условий лицензионного соглашения

5. Выбрать путь для установки приложения или оставить путь, предлагаемый по умолчанию, и нажать кнопку «Далее» (см. рисунок 20).

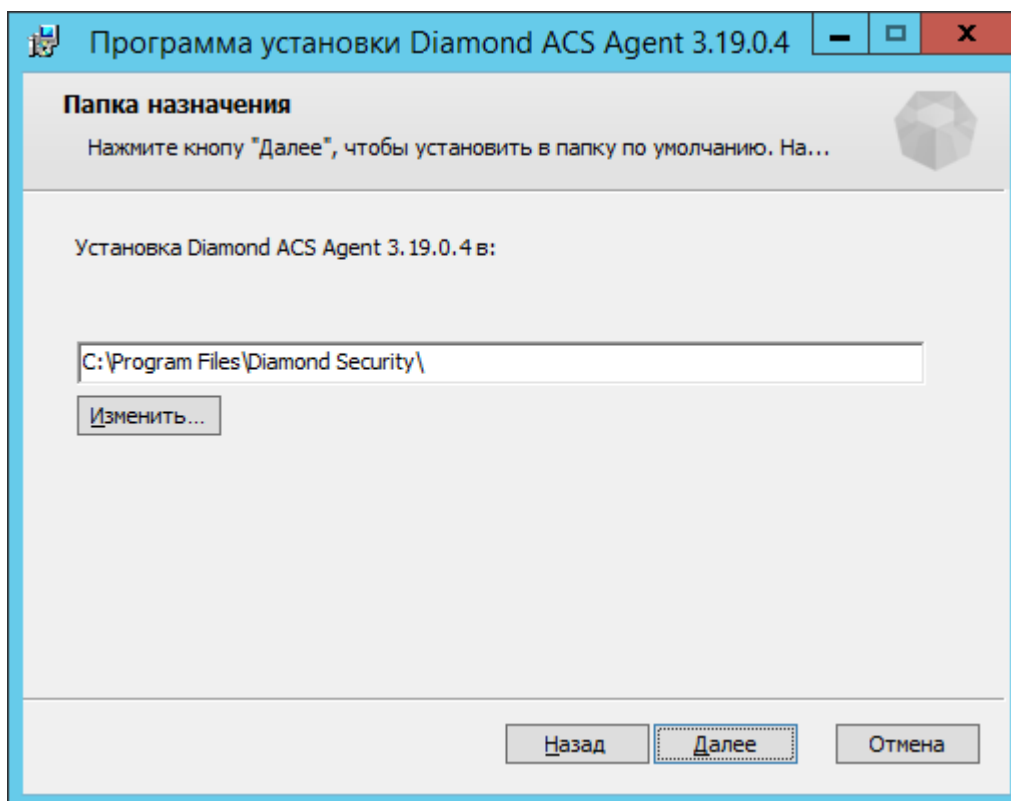


Рисунок 20 – Окно выбора пути установки

6. Нажать кнопку «Установить» (см. рисунок 21).

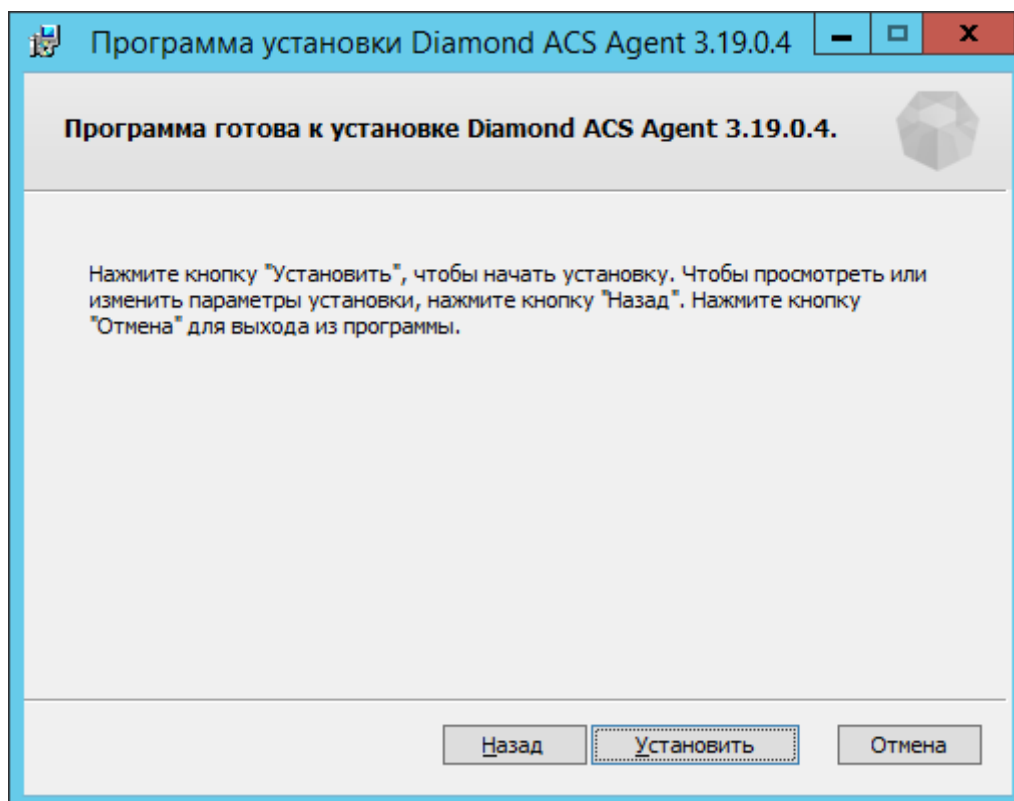


Рисунок 21 – Окно выбора пути установки



7. Дождаться окончания установки и нажать кнопку «Готово» (см. рисунок 22).

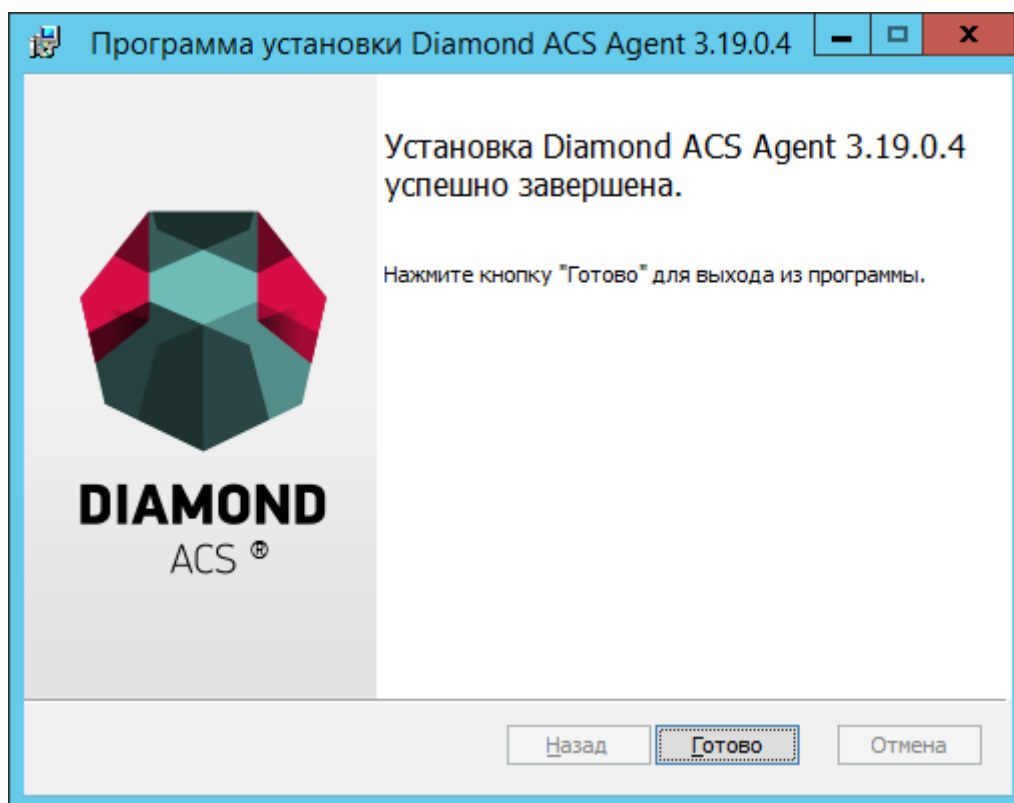


Рисунок 22 – Положение кнопки «Готово»

8. Выполнить перезагрузку ОС, установленной на АРМ (см. рисунок 23).

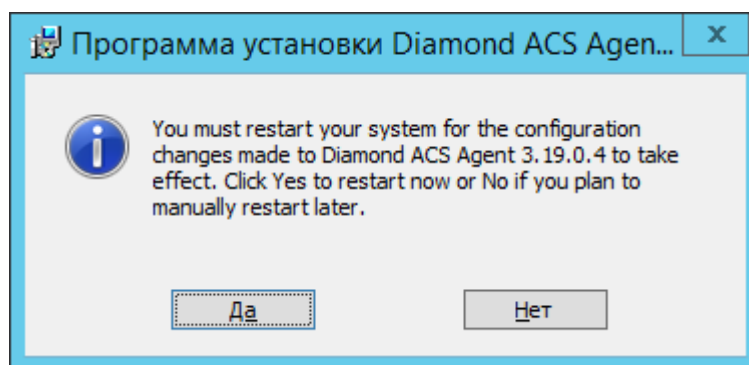


Рисунок 23 – Окно принятия решения о перезагрузке

Внимание! Работа агента возможна только после перезагрузки компьютера, т.к. необходимые службы будут запущены при следующем старте операционной системы. Перезагрузку компьютера можно отложить и это никак не повлияет на текущую работу пользователя и используемые приложения.



3.7.2 Установка на АРМ с ОС семейства Linux

Для установки приложения «Diamond ACS Agent Workstation Net» на АРМ с установленными ОС семейства Linux (данные АРМ должны находиться в домене Windows) необходимо:

1. Запустить программу инсталляции приложения «Diamond ACS Agent Workstation Net» (DmAgent.sh) на защищаемом АРМ.
2. От имени суперпользователя (root) выполнить команду:
3. # ./diamond-agent-installer.sh

Примечание: скрипт установки «diamond-agent-installer.sh» написан для семейства ОС Linux Ubuntu. В случае если на Вашем дистрибутиве Linux он работает некорректно, необходимо обратиться к разработчику.

4. Инсталлятор автоматически определит версию используемого дистрибутива Linux и установит соответствующие системные компоненты.
5. Ввести имя доменного пользователя и его пароль, который «Diamond ACS Agent Workstation Net» будет использовать для подключения к «Active Directory». Данный пользователь должен иметь права записи в объект Computer данного АРМ и права чтения на все остальные объекты.
6. После завершения инсталляции выполнить перезагрузку ОС, установленной на АРМ.



4 Активация «Diamond ACS»

В СКРД «Diamond ACS» используется сетевая модель лицензирования, то есть ограничивается взаимодействие между модулями, а также настройка и мониторинг СКРД. Лицензия выдается на определенный срок и на определенное количество программных модулей одного типа в пределах одного домена. Общее количество модулей, на которое рассчитана одна лицензия, можно распределить между несколькими серверами безопасности «Diamond ACS» в пределах одного домена.

По умолчанию, то есть без активной настроенной лицензии, в СКРД «Diamond ACS» разрешено подключение только «Diamond ACS Security Manager» и «Security Monitor» к серверу безопасности «Diamond ACS Security Server» с использованием адреса «localhost» (модули управления и мониторинга должны быть установлены в той же ОС и на том же компьютере, что и сервер безопасности «Diamond ACS»). Настройка политик безопасности становится возможной только при соблюдении следующих условий:

- имеется активная (не истекшая по сроку) серверная лицензия, сохраненная в AD и назначенная тому серверу безопасности, к которому подключен «Diamond ACS Security Manager»;
- количество установленных в домене серверов безопасности не превышает количества серверов, указанного в активных лицензиях для данного домена.

Установка приложения «Diamond ACS Agent Workstation Net» возможна, если количество установленных в домене агентов меньше количества агентов, указанного в активных лицензиях для данного домена.

При истечении срока лицензии для агентов модули «Diamond ACS Agent Workstation Net» продолжают использовать полученные политики безопасности на АРМ, но их централизованное управление и мониторинг становятся невозможными. При истечении срока серверной лицензии поведение сервера безопасности «Diamond ACS Security Server» будет идентично работе без лицензии (см. выше).

В сети интернет работает WEB-сервис для автоматизированного получения лицензий. Адрес страницы: <http://office.tssltd.ru>.

Процесс активации СКРД «Diamond ACS» включает в себя следующие шаги:



1. Установка «Diamond ACS Security Server» (см. подраздел 3.5).
2. Установка «Diamond ACS Security Manager» и «Security Monitor» на компьютер, на котором установлен «Diamond ACS Security Server» (см. подраздел 3.6).
3. Подключение с помощью «Diamond ACS Security Manager» к серверу безопасности, используя в качестве имени сервера безопасности «localhost» (см. подраздел 5.2).
4. Запрос нужного типа и требуемого количества лицензий для каждого домена (см. п. 5.3.1).
5. Отправка запроса в САВЛ (см. подраздел 4.2).
6. Получение сгенерированной лицензии (см. подраздел 4.3).
7. Импорт полученной лицензии в СКРД «Diamond ACS» (см. п. 5.3.2).
8. Распределение лицензий по серверам безопасности (см. п. 5.3.3).
9. Установка «Diamond ACS Agent Workstation Net» на защищаемые АРМ (см. подраздел 3.7).

4.1 Регистрация в системе автоматической выдачи лицензий

Регистрация возможна только при наличии инвайт-кода, который выдается заказчику сотрудником фирмы-разработчика или зарегистрированным в данной системе дистрибьютором.

Для регистрации в САВЛ необходимо выполнить следующие действия:

1. Зайти на главную страницу САВЛ (<http://office.tssltd.ru>) (см. рисунок 24).

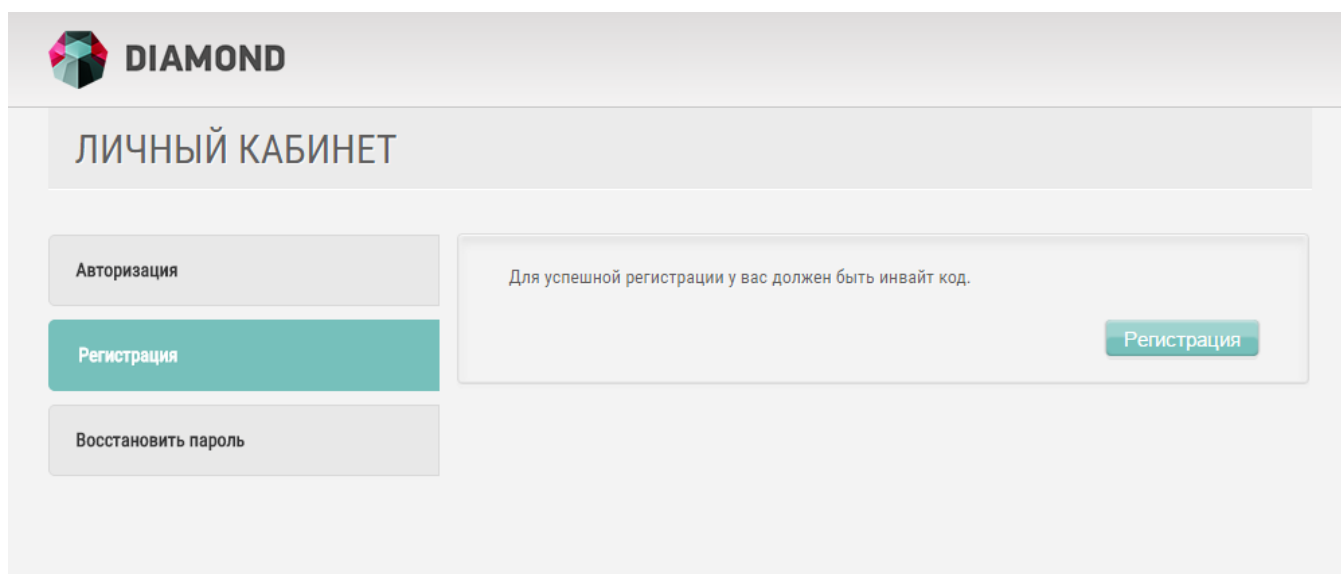


Рисунок 24 – Главная страница САВЛ



DIAMOND

СКРД Diamond ACS. Инструкция по настройке и эксплуатации

2. Выбрать пункт «РЕГИСТРАЦИЯ».
3. Заполнить регистрационные данные (см. рисунок 25).



DIAMOND



DIAMOND

РЕГИСТРАЦИЯ

Логин: *

Пароль: *

Повторите пароль: *

Адрес электронной почты: *

Повторите адрес электронной почты: *

Инвйт код: *

КОНТАКТНЫЕ ДАННЫЕ

Ваше Ф.И.О.: *

Контактный адрес: *

Контактный адрес: *

Контактный телефон: *

Регистрация

Рисунок 25 – Окно регистрации

4. Нажать кнопку регистрация.



В случае успешной регистрации отобразится страница с подтверждением и будет отправлено письмо на указанный адрес электронной почты.

4.2 Отправка запроса на получение лицензии

Перед отправкой запроса на получение лицензии необходимо выполнить вход в систему автоматической выдачи лицензий (регистрация описана в подраздел 4.1). Для отправки запроса на получение лицензии на приобретенное ПО необходимо:

1. Зайти на главную страницу системы автоматической выдачи лицензий (САВЛ).
2. Авторизоваться зарегистрированным пользователем (см. рисунок 26).

The screenshot shows the 'ЛИЧНЫЙ КАБИНЕТ' (Personal Cabinet) page of the DIAMOND system. On the left side, there is a vertical menu with three buttons: 'Авторизация' (Authorization) in a teal color, 'Регистрация' (Registration), and 'Восстановить пароль' (Reset password). The main content area contains a login form with two input fields: 'Имя пользователя: *' (Username) and 'Пароль: *' (Password). Both fields have placeholder text: 'Введите ваше имя пользователя' and 'Введите ваш пароль'. A teal 'Войти' (Login) button is positioned at the bottom right of the form.

Рисунок 26 – Окно авторизации

3. Выбрать пункт меню «ДЕЙСТВИЯ» → «Договоры» (см. рисунок 27).



The screenshot shows the DIAMOND web interface. At the top left is the DIAMOND logo. To its right are navigation links: 'НА ГЛАВНУЮ', 'ДЕЙСТВИЯ', and 'ВЫЙТИ'. The 'ДЕЙСТВИЯ' menu is open, showing 'Договоры' (highlighted) and 'Запросы'. Below the navigation is a 'ГЛАВНАЯ' header. The main content area displays a greeting: 'Здравствуйте, [Имя Фамилия]'. It then lists the service organization: 'Вас обслуживает организация:' followed by a table with details for 'ООО "ТСС"'. Below this is another section for the personal manager: 'Ваш личный менеджер:' followed by a table with details for 'Ибрагимов, Александр Александрович'.

Вас обслуживает организация:	
Название организации:	ООО "ТСС"
Контактный адрес:	Борисовская д. 1 этаж 9
Контактный телефон:	8-(495)-943-08-03

Ваш личный менеджер:	
ФИО:	Ибрагимов, Александр Александрович
Контактный адрес:	105318, г. Москва, ул. Ибрагимова, д. 31, офис 800
Контактный телефон:	(495) 943 08 03

Рисунок 27 – Положение вкладок «ДЕЙСТВИЯ» → «Договоры»



4. Выбрать необходимый договор нажатием на кнопке «+» (см. рисунок 28).

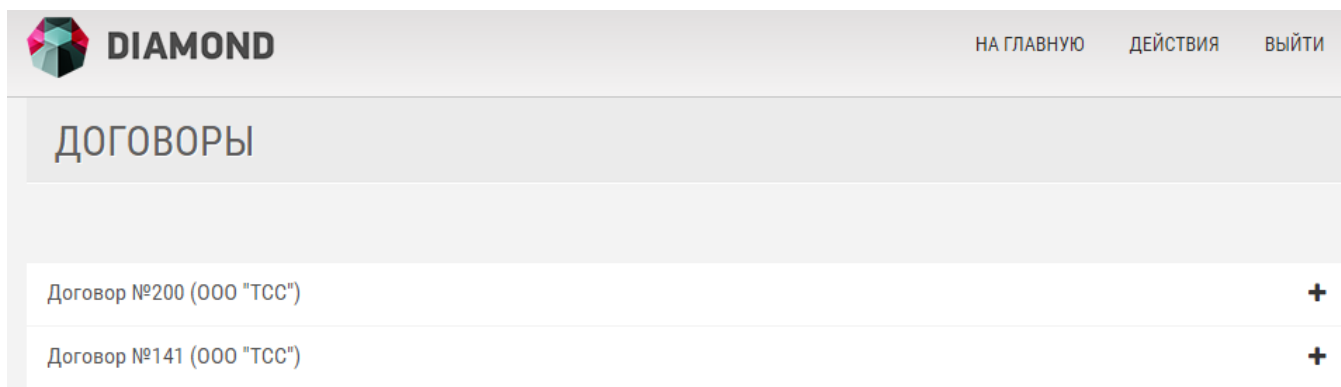


Рисунок 28 – Окно выбора договора

5. Нажать на кнопку «СДЕЛАТЬ ЗАПРОС», расположенную под таблицей (см. рисунок 29).



Договор №200 (ООО «ТСС»)

Создал:
Создан: 2015-12-02 18:13:08
Действует до: 2019-12-01 00:00:00
Утверждена: Да

Продукты:

Имя продукта	Количество	Запрошено	Осталось
Diamond ACS сервер, сетевой вариант	10000	125	9875
Diamond ACS консоль конфигурирования и мониторинга, сетевой вариант	10000	130	9870
Diamond ACS агент для серверов WINDOWS, сетевой вариант	10000	160	9840
Diamond ACS агент для рабочих станций WINDOWS, сетевой вариант	10000	171	9829
Diamond ACS агент для LINUX, сетевой вариант	10000	36	9964
Diamond ACS агент для SOLARIS, сетевой вариант	10000	35	9965
Diamond ACS агент для FREEBSD и OPENBSD, сетевой вариант	10000	35	9965
Diamond ACS VPN построитель, сетевой вариант	10000	45	9955
Diamond ACS консоль конфигурирования и мониторинга, автономный вариант	10000	22	9978
Diamond ACS агент для серверов WINDOWS, автономный вариант	10000	2	9998
Diamond ACS агент для рабочих станций WINDOWS, автономный вариант	10000	7	9993

Сделать запрос

Рисунок 29 – Положение кнопки «Сделать запрос»

6. Выбрать созданный ранее файл запроса.
7. Нажать кнопку «ЗАПРОСИТЬ» (см. рисунок 30).



DIAMOND

НА ГЛАВНУЮ ДЕЙСТВИЯ ВЫЙТИ

Запрос будет произведен по договору №200.

Выберите файл Файл не выбран

Запросить

Рисунок 30 – Положение кнопки «Запросить»



4.3 Получение запрошенных лицензий

Для получения запрошенных лицензий необходимо:

1. Зайти на главную страницу системы автоматической выдачи лицензий.
2. Выбрать пункт «ДЕЙСТВИЯ» → «Запросы» (см. рисунок 31).

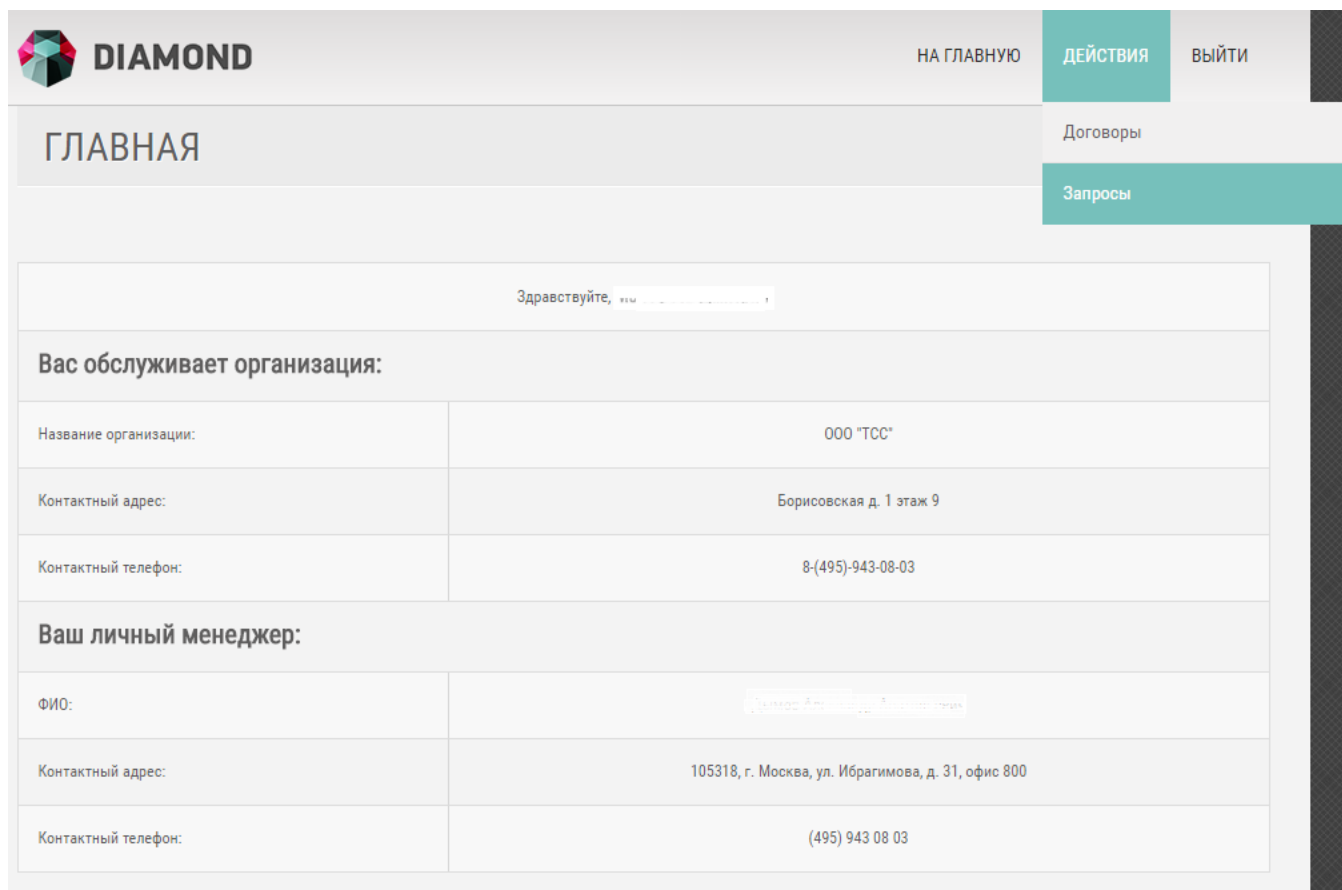


Рисунок 31 – Положение вкладок «ДЕЙСТВИЯ» → «Запросы»

3. Выбрать необходимый запрос нажатием на кнопке «+».
4. Нажать на кнопку «СКАЧАТЬ», расположенную под таблицей.

В результате пользователю предоставлен файл с запрошенными лицензиями с расширением *.lresp (см. рисунок 32).



DIAMOND



ЗАПРОСЫ

1 2 3 4

Договор №200 (sub.diamondacs-demo.local.lreq)

Создал: [Александр Димитрия](#)

Создан: 2016-03-29 13:52:10

Действует до: 2019-12-01 00:00:00

Продукты:

Имя продукта	Серийный Номер	Количество
Diamond ACS сервер, сетевой вариант	00NZ-00ER-0KNV-00B7-FSA6	5
Diamond ACS консоль конфигурирования и мониторинга, сетевой вариант	00NW-00EK-0KN6-00A6-CJ4H	5
Diamond ACS агент для серверов WINDOWS, сетевой вариант	00NF-00JX-0KNN-00CP-G10D	10
Diamond ACS агент для рабочих станций WINDOWS, сетевой вариант	00NM-00J0-0KN2-00AC-BVB9	10

Скачать



4.4 Обновление лицензии СКРД «Diamond ACS»

По истечении срока лицензии необходимо обновить для полноценного функционирования СКРД «Diamond ACS».

Процесс обновления лицензий СКРД «Diamond ACS» состоит из следующих шагов:

1. Создание запроса лицензий (см. п. 5.3.1).
2. Отправка запроса в САВЛ (см. подраздел 4.2).
3. Получение сгенерированной лицензии (см. подраздел 4.3).
4. Импорт полученной лицензии в СКРД «Diamond ACS» (см. п. 5.3.2).

Все этапы идентичны первичной активации продукта. После импорта новых лицензий в СКРД «Diamond ACS» можно удалить старые лицензии, срок действия которых уже истек.



Приложение служит для настройки СКРД «Diamond ACS». Основные функции приложения «Diamond ACS Security Manager»:

- построение топологии серверов и агентов СКРД «Diamond ACS» в закрытом контуре;
- настройка политик безопасности на защищаемых АРМ;
- настройка контроля целостности ресурсов;
- настройка сбора и хранения журналов, защищаемых АРМ;
- назначение электронных идентификаторов пользователям;
- задание паролей для авторизации при использовании в комплексе аппаратного модуля «Diamond ACS HW»;
- управление лицензиями СКРД «Diamond ACS».

5.1 Основные принципы работы

Для подключения к серверу безопасности необходимо указать IP-адрес или DNS-имя сервера с установленным приложением «Diamond ACS Security Server». Доступ к изменению политик безопасности «Diamond ACS» предоставляется только членам групп: «Администраторы домена» и «Diamond-Admins». Имя пользователя и адрес сервера безопасности, указанные при аутентификации, автоматически сохраняются при входе в главное окно приложения.

Если СКРД «Diamond ACS» не активирован, то при попытке аутентификации с компьютера, отличного от того, на котором установлен сервер безопасности, появится сообщение об ошибке: «Для вызываемой службы действует лицензия на определенное число подключений...». В этом случае необходимо выполнить активацию (см. п. 4).

Для оптимизации работы приложения «Diamond ACS Security Manager» с несколькими доменами в одном лесу данные загружаются либо при разворачивании элемента соответствующего домена, либо при нажатии кнопки «Перечитать». Автоматическую загрузку данных можно настроить, поставив отметку в меню «Файл» рядом с пунктом «Загружать все при запуске».

Выбирая элементы домена двойным нажатием левой клавиши мыши (или клавишей «Enter»), можно просмотреть и изменить их настройки.



Для сохранения всех внесенных изменений необходимо нажать кнопку «Сохранить», находящуюся слева на панели инструментов главного окна «Diamond ACS Security Manager». В случае если внесенные изменения не были сохранены, перед выходом из «Diamond ACS Security Manager» (или при нажатии на кнопку «Перечитать») администратору безопасности будет предложено сохранить все изменения.

При сохранении изменений в первый раз поле «Контроллер домена» пустое и не требует заполнения. Если его заполнить, то при последующих сохранениях изменений оно будет автоматически подставляться.

Возможно одновременное подключение к серверу безопасности «Diamond ACS» с нескольких Security Manager & Monitor, запущенных на разных компьютерах, согласно приобретенному количеству лицензий с типом «Программы управления». Количество лицензий с типом «Программы управления» определяет максимальное количество компьютеров, с которых можно подключиться к серверу безопасности.

Если необходимо иметь пользователя с полномочиями только на просмотр политик безопасности без возможности сохранения настроек, то в Active Directory необходимо средствами оснастки Windows «Пользователи и компьютеры» создать группу безопасности «Diamond-Users» и требуемого доменного пользователя сделать членом этой группы. Используя имя и пароль доменного пользователя, являющегося членом группы «Diamond-Users», с помощью Security Manager можно подключиться к серверу безопасности. При попытке сохранения внесенных изменений под этой учетной записью выдается сообщение о невозможности сохранения настроек со списком изменений, которые не удалось сохранить. Также члены группы могут подключаться к серверу безопасности с помощью Security Monitor и при этом нет никаких ограничений на выполняемые действия. Реализована поддержка вложенности групп, т.е. если доменная учетная запись является членом группы, которая является членом группы «Diamond-Users», то будет разрешено подключение к серверу безопасности.

В иерархии при выборе объекта через контекстное меню доступно изменение свойств всех дочерних агентов или пользователей, являющихся членами подразделений (OU) и групп (Groups). В случае с подразделениями реализована вложенность, т.е. будут выбраны все дочерние элементы вниз по дереву от текущего выбранного подразделения. Для групп



вложенность не реализована и будут выбраны пользователи или компьютеры на первом дочернем уровне иерархии.

5.2 Интерфейс

5.2.1 Главное окно программы

Главное окно программы «Diamond ACS Security Manager» изображено на рисунке 33.

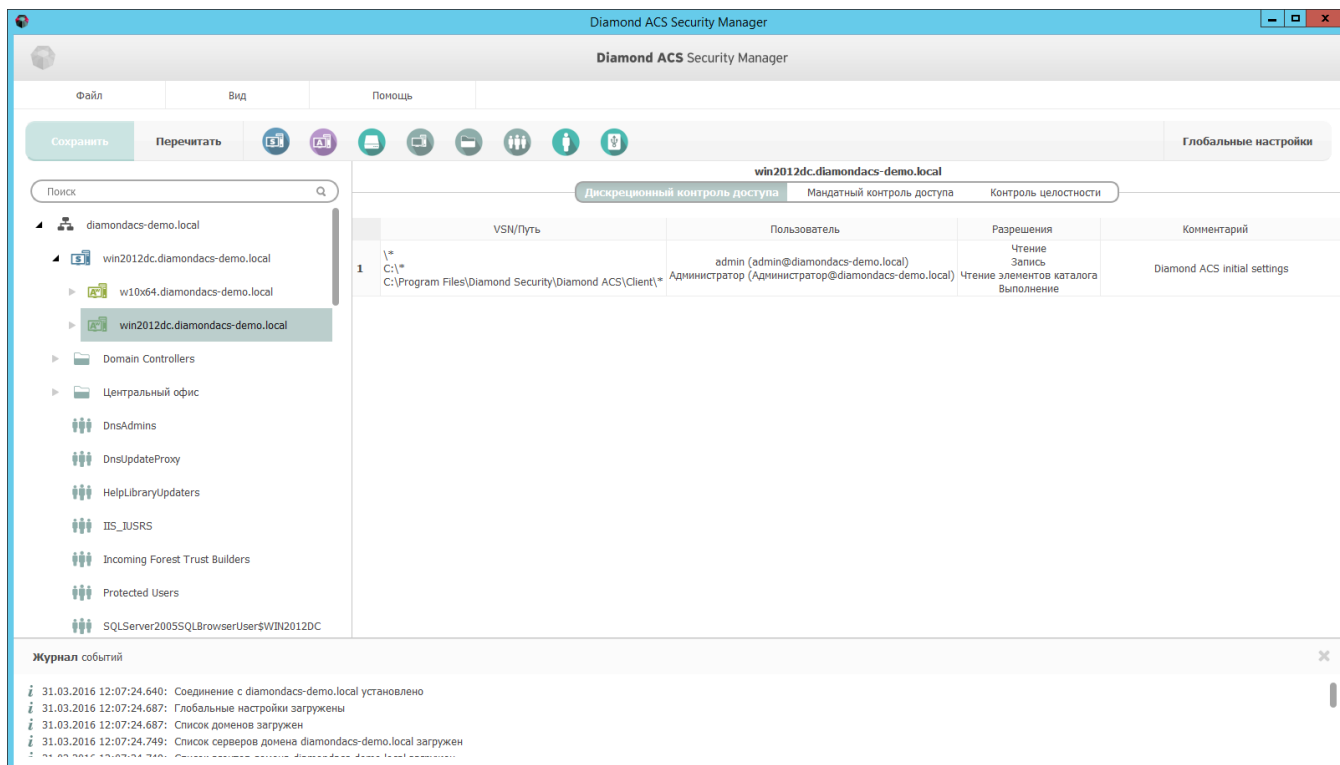


Рисунок 33 – Главное окно приложения «Diamond ACS Security Manager»

- 1 Главное меню
- 2 Панель инструментов
- 3 Иерархия
- 4 Правила контроля
- 5 Журнал событий



5.2.2 Главное меню

Главное меню программы «Diamond ACS Security Monitor» изображено на рисунке 34. Подробное описание вкладок отображено в таблицах 1, 2, 3. Положение вкладок отображено на рисунках 35, 36, 37.

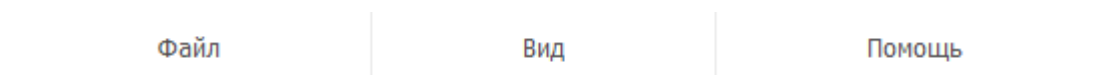


Рисунок 34 – Главное меню

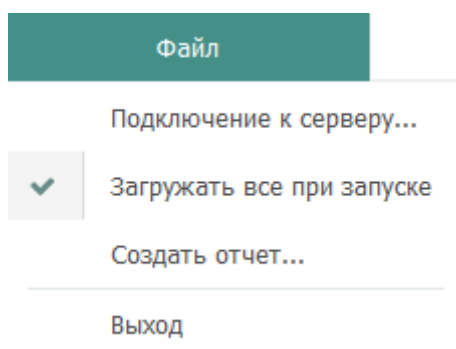


Рисунок 35 – Меню «Файл» приложения «Diamond ACS Security Manager»

Таблица 1 – Описание меню «Файл».

Подключение к серверу...	Отображает окно для подключения к серверу безопасности
Загружать все при запуске	Производит загрузку иерархии домена и всех настроек политик безопасности при подключении к серверу безопасности
Создать отчет...	Отображает окно мастера создания отчетов со сведениями о: <ul style="list-style-type: none">• ресурсах, объектах, параметрах защищаемых компьютеров;• пользователях;• персональных идентификаторах;• съемных носителях информации.



Выход	Завершение работы программы
--------------	-----------------------------

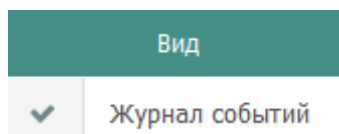


Рисунок 36 – Меню «Вид» приложения «Diamond ACS Security Manager»

Таблица 2 – Описание меню «Вид».

Журнал событий	Отобразить/скрыть журнал событий
-----------------------	----------------------------------

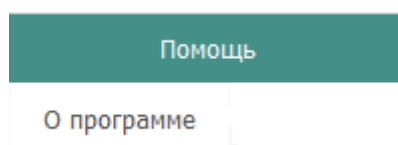


Рисунок 37 – Меню «Помощь» приложения «Diamond ACS Security Manager»

Таблица 3 – описание меню «Помощь»

Помощь	Отображает информацию о разработчике и версию продукта.
---------------	---------------------------------------------------------

5.2.3 Панель инструментов

Панель инструментов изображена на рисунке 38. Описание кнопок «Сохранить» и «Перечитать» отображено в таблице 4.



Рисунок 38 – Панель инструментов приложения «Diamond ACS Security Manager»

Таблица 4 – Описание кнопок «Сохранить» и «Перечитать».



Сохранить	Записать произведенные в конфигурации изменения в AD
Перечитать	Отмена внесенных в конфигурацию изменений и загрузка текущей конфигурации



Скрыть/отобразить сервера безопасности



Скрыть/отобразить АРМ с установленным приложением «Diamond ACS Agent Workstation Net»



Скрыть/отобразить VPN построители



Скрыть/отобразить подразделения



Скрыть/отобразить группы пользователей



Скрыть/отобразить пользователей



Скрыть/отобразить зарегистрированные съемные накопители



Скрыть/отобразить АРМ без установленных приложений «Diamond ACS Agent Workstation Net» и «Diamond ACS Security Server»

5.3 Управление лицензиями

Описание модели лицензирования, процесса активации и общего порядка действий, необходимых для активации СКРД «Diamond ACS» приведено в разделе Активация «Diamond ACS».

5.3.1 Создание запроса

Для создания запроса на получение лицензии необходимо осуществить следующие действия:

1. В разделе «Иерархия» вызвать контекстное меню для активируемого домена.
2. В контекстном меню выбрать пункт «Лицензии».
3. В окне лицензий нажать кнопку «Запрос» (см. рисунок 39).



4. В окне запроса лицензий указать в соответствующих позициях купленное количество лицензий (см. рисунок 40).
5. Указать расположение директории, в которой будет создан файл запроса.
6. Нажать кнопку «Создать».

Описание окна «Лицензии» отображено в таблице 5. Описание окна запроса лицензий отображено в таблице 6.

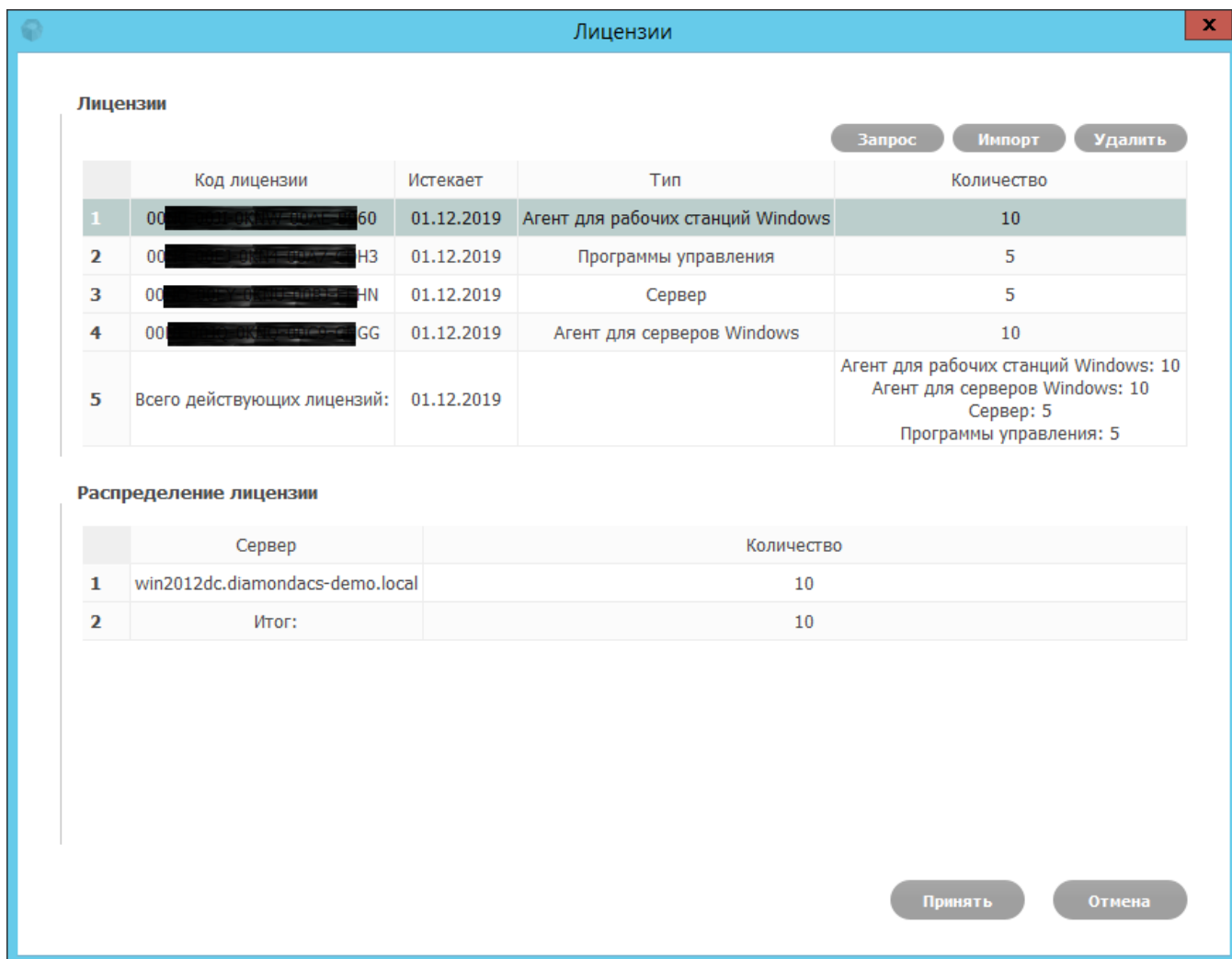


Рисунок 39 – Окно лицензий приложения «Diamond ACS Security Manager»

Таблица 5 – Описание окна «Лицензии».

Лицензии	
Код лицензии	Уникальный номер лицензии



DIAMOND

Истекает	Дата окончания срока действия лицензии
Тип	Тип поддерживаемых лицензией модулей
Количество	Количество поддерживаемых лицензией модулей
Распределение лицензий	
Сервер	Сервер безопасности
Количество	Количество модулей, разрешенных для подключения к серверу



Запрос лицензий

Пожалуйста, задайте необходимое количество для каждого типа лицензий.
Если нужно, введите здесь свои комментарии

Тип	Количество
VPN	0
Агент для BSD	0
Агент для Linux	0
Агент для Solaris	0
Агент для рабочих станций Windows	1
Агент для серверов Windows	1
Программы управления	1
Сервер	1

Открыть содержащую объект папку



Рисунок 40 – Окно запроса лицензий приложения «Diamond ACS Security Manager»

Таблица 6 – Описание окна запроса лицензий.

VPN	Лицензия на VPN построитель «Diamond ACS VPN/FW»
Агент для BSD	Лицензия на «Diamond ACS Workstation Net» для ОС семейства BSD
Агент для Linux	Лицензия на «Diamond ACS Workstation Net» для ОС семейства Linux
Агент для Solaris	Лицензия на «Diamond ACS Workstation Net» для ОС семейства Solaris
Агент для рабочих станций Windows	Лицензия на клиентскую версию «Diamond ACS Workstation Net» для ОС семейства Windows
Агент для серверов Windows	Лицензия на серверную версию «Diamond ACS Workstation Net» для ОС семейства Windows
Программы управления	Лицензия на подключения к серверу модулей «Diamond ACS Security Monitor» и «Diamond ACS Security Manager»
Сервер	Лицензия на сервер безопасности «Diamond ACS Security Server»

5.3.2 Импорт лицензий

Для импорта лицензий в СКРД «Diamond ACS» необходимо выполнить следующие действия:



1. В разделе «Иерархия» вызвать контекстное меню для лицензируемого домена.
2. В контекстном меню выбрать пункт «Лицензии».
3. В окне лицензий нажать кнопку «Импорт».
4. Выбрать файл ответа и нажать кнопку «Открыть».
5. Нажать кнопку «Принять».
6. Нажать кнопку «Сохранить» на панели инструментов.

5.3.3 Распределение лицензий

Для распределения лицензий в СКРД «Diamond ACS» необходимо выполнить следующие действия:

1. В разделе «Иерархия» вызвать контекстное меню для лицензируемого домена.
2. В контекстном меню выбрать пункт «Лицензии».
3. В поле «Лицензии» открывшегося окна лицензий выбрать необходимую лицензию.
4. В поле «Распределение лицензий» дважды кликнуть на позиции «Количество» необходимого сервера безопасности.
5. Указать необходимое количество лицензий.
6. Нажать кнопку «Принять».

Если общее число соединений по серверам (строка «Итог») превышает количество соединений, на которое рассчитана лицензия, то появится предупреждение о неправильном распределении (см. рисунок 41).

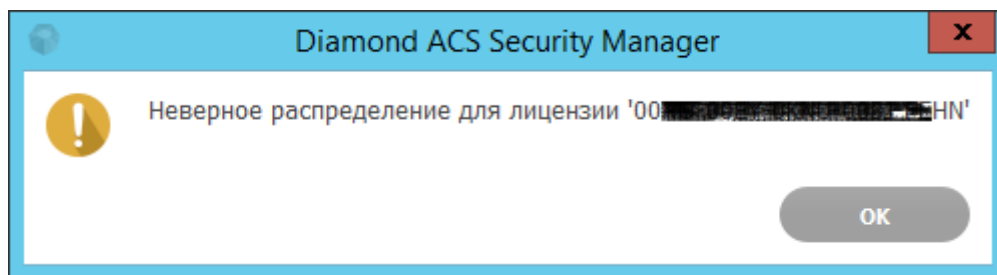


Рисунок 41 – Предупреждение о неправильном распределении лицензий

5.3.4 Удаление лицензий

Для удаления лицензий из СКРД «Diamond ACS» необходимо выполнить следующие действия:

1. В разделе «Иерархия» вызвать контекстное меню для лицензируемого домена.



2. В контекстном меню выбрать пункт «Лицензии».
3. В поле «Лицензии» открывшегося окна лицензий выбрать необходимую лицензию.
4. Нажать кнопку «Удалить».
5. Нажать кнопку «Принять».
6. Нажать кнопку «Сохранить» на панели инструментов.

5.4 Настройка сетевых параметров

5.4.1 Настройка порта сервера безопасности

Для настройки порта сервера безопасности необходимо выполнить следующие действия:

1. Во вкладке «Иерархия» вызвать контекстное меню для настраиваемого сервера безопасности (см. рисунок 42).
2. В контекстном меню выбрать пункт «Свойства».
3. Установить необходимое значение порта в поле «Слушающий порт».
4. Нажать кнопку «Принять».

Описание контекстного меню отображено в таблице 7.

Примечание: в случае изменения слушающего порта на отличный от 8030, порт соединения нужно будет явно указывать в поле «Сервер безопасности» окна подключения.



Настройки сервера - win2012dc.diamondacs-demo.local

Основные SMTP

Подчинение серверу в родительском домене

Изменить Сбросить

Слушающий порт 8030 ▲ ▼

Интервал опроса службы каталогов (мин) 1 ▲ ▼

Принять Отмена



Рисунок 42 – Вкладка «Основные» окна настроек сервера безопасности

Таблица 7 – Описание вкладки основные окна настроек сервера безопасности.

Подчинение серверу в родительском домене	Сервер безопасности, для которого текущий сервер будет дочерним в иерархии
Слушающий порт	TCP-порт для подключения к серверу
Интервал опроса службы каталогов	Интервал опроса Active Directory сервером безопасности

5.4.2 Настройка интервала опроса Active Directory

Конфигурация СКРД «Diamond ACS» хранится в AD. Изменения в конфигурации проверяются серверами безопасности и клиентскими АРМ с заданной в минутах периодичностью. При настройке иерархии клиентские АРМ получают только изменившиеся параметры конфигурации и только от того сервера безопасности, к которому подключены (подчинены в иерархии).

Для настройки интервала опроса сервером безопасности службы каталогов необходимо выполнить следующие действия:

1. Во вкладке «Иерархия» вызвать контекстное меню для настраиваемого сервера безопасности.
2. В контекстном меню выбрать пункт «Свойства».
3. Установить необходимое значение интервала в поле «Интервал опроса службы каталогов».
4. Нажать кнопку «Принять».

Для настройки интервала опроса клиентским АРМ службы каталогов необходимо выполнить следующие действия:

1. Во вкладке «Иерархия» вызвать контекстное меню для настраиваемого клиентского АРМ.
2. В контекстном меню выбрать пункт «Свойства».
3. Установить необходимое значение интервала в поле «Интервал опроса службы



DIAMOND

СКРД Diamond ACS. Инструкция по настройке и эксплуатации

каталогов».

4. Нажать кнопку «Принять».



Приложение служит для просмотра событий, связанных с безопасностью сети, а также для корреляции их с другими системными событиями. Позволяет подключаться к одному из серверов безопасности и получать информацию о его состоянии и происходящих на нем событиях, а также аналогичную информацию по всем рабочим станциям и серверам, подчиненным данному серверу согласно заданной в «Diamond ACS Security Manager» топологии.

Также приложение позволяет в реальном времени отслеживать такие события, как НСД и нарушение целостности данных; имеется возможность блокировки, перезагрузки и отключения рабочих станций.

Без настроенной иерархии подчинения агентов серверу безопасности агенты не будут отображаться в Мониторе.

По умолчанию при выборе в иерархии некоторого АРМ для него запрашивается: общая информация, информация о нарушениях контроля целостности, журналы «Diamond ACS», «Приложение», «Система», «Безопасность» за текущие сутки (без предварительной синхронизации, и, если ранее не были загружены в приложение).

В случае если АРМ не подключен к серверу (например, если не загружена ОС, или отсутствует сетевое подключение), то соответствующая ему пиктограмма отображается серым цветом, а в поле «Статус» вкладки «Информация» присутствует запись «остановлен».

Основным журналом безопасности в СКРД «Diamond ACS» является журнал «Diamond ACS», создаваемый на клиентских АРМ при установке модуля «Diamond ACS Agent Workstation Net».

6.1 Запуск, идентификация и аутентификация

Для начала работы в приложении «Diamond ACS Security Monitor» необходимо выполнить следующие действия:

1. Запустить программу «SecurityMonitor.exe».
2. После появления окна подключения ввести логин и пароль администратора домена или члена группы «Diamond-Admins».



СКРД Diamond ACS. Инструкция по настройке и эксплуатации

3. Ввести доменное имя или IP-адрес сервера безопасности.
4. Нажать кнопку «Вход» (см. рисунок 43).
5. Если все введенные данные верны, то окно аутентификации закроется и появится главное окно приложения (см. рисунок 44).

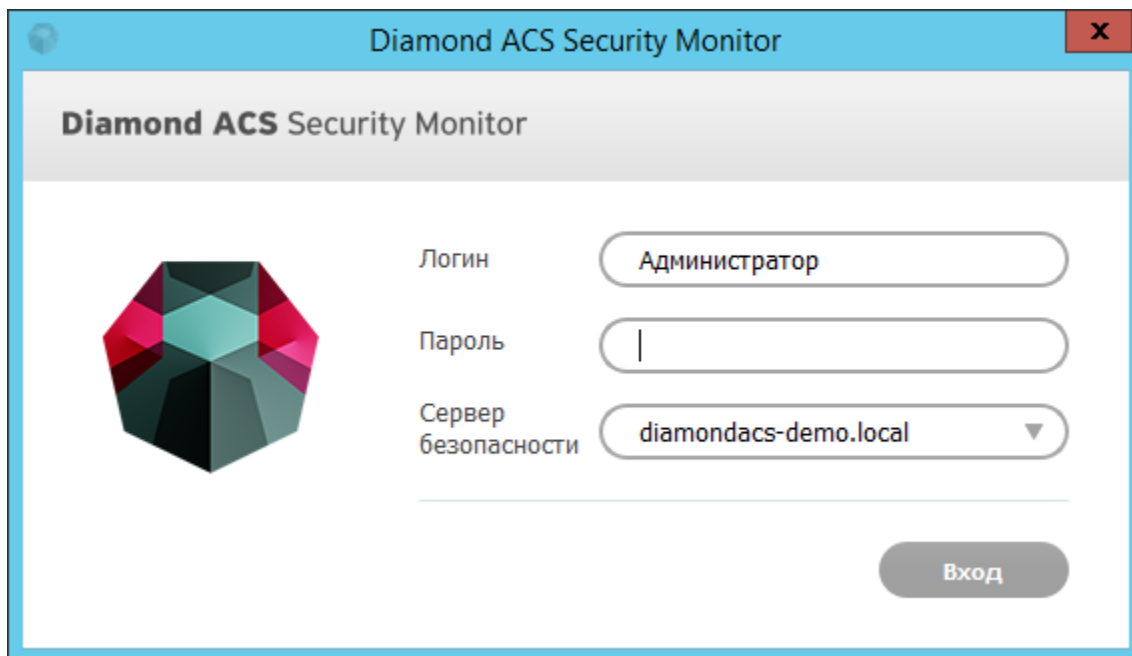


Рисунок 43 – Окно входа в систему

Описание окна входа в систему отображено в таблице 8.

Таблица 8 – Окно входа в систему.

Логин	Логин администратора сервера безопасности
Пароль	Пароль администратора сервера безопасности
Сервер безопасности	DNS имя или IP-адрес сервера безопасности

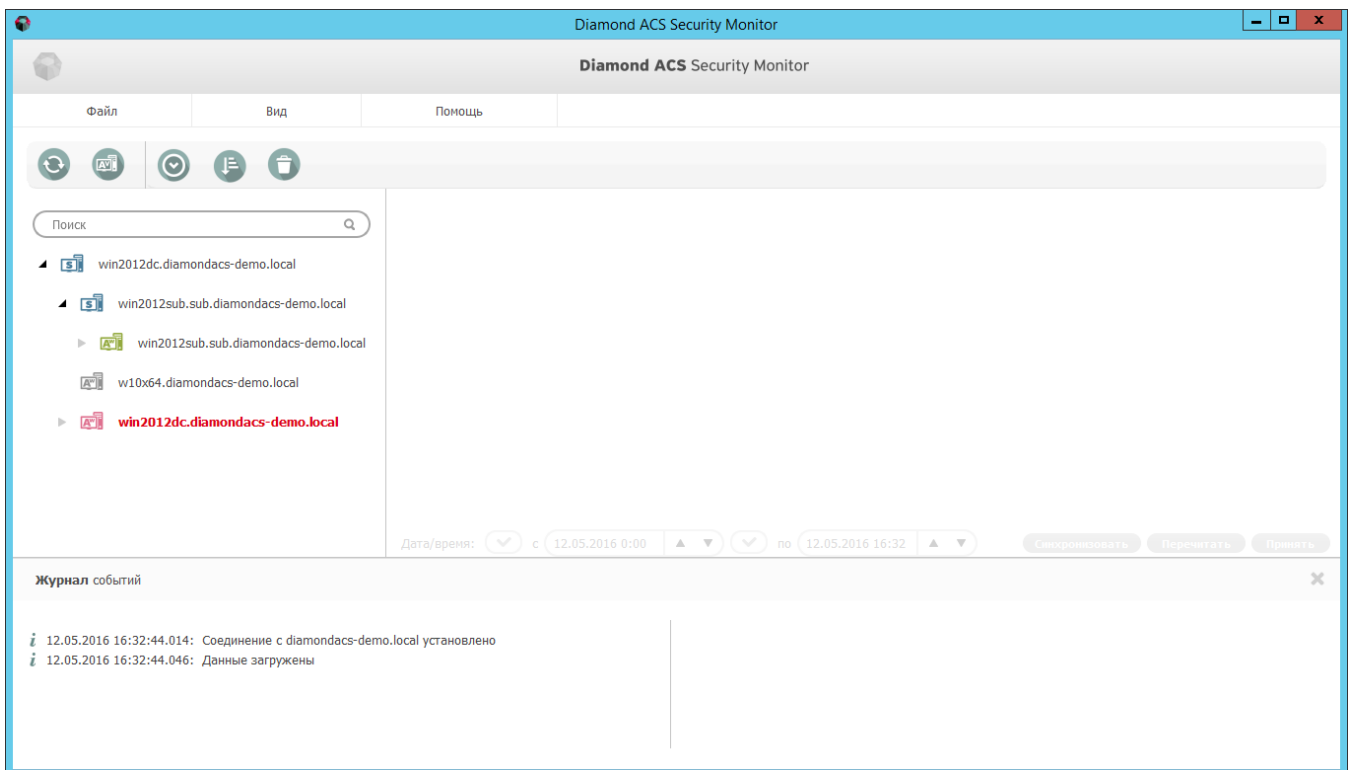


Рисунок 44 – Главное окно приложения «Diamond ACS Security Monitor»








6.2 Панель инструментов

Панель инструментов изображена на рисунке 45. Описание кнопок на инструментальной панели главного окна приложения отображено в таблице 9.



Рисунок 45 - Панель инструментов приложения «Diamond ACS Security Monitor»

Таблица 9 – Описание инструментальной панели главного окна приложения.

 Перечитать	Запрос актуального состояния системы
 Показать версии агентов	Отображает версии установленных агентов на компьютерах клиентов
 Автопрокрутка журнала событий	При возникновении новых событий происходит автоматическая прокрутка в окне и отображение последних по времени событий.
 Циклическая перезапись журнала событий	При достижении определенного размера журнала новые события будут перезаписывать старые
 Очистить журнал событий	Стирает все событий в журнале

6.3 Окно мониторинга версий агентов

Окно мониторинга версий агентов изображено на рисунке 46. Описание окна мониторинга версий агентов отображено в таблице 10.

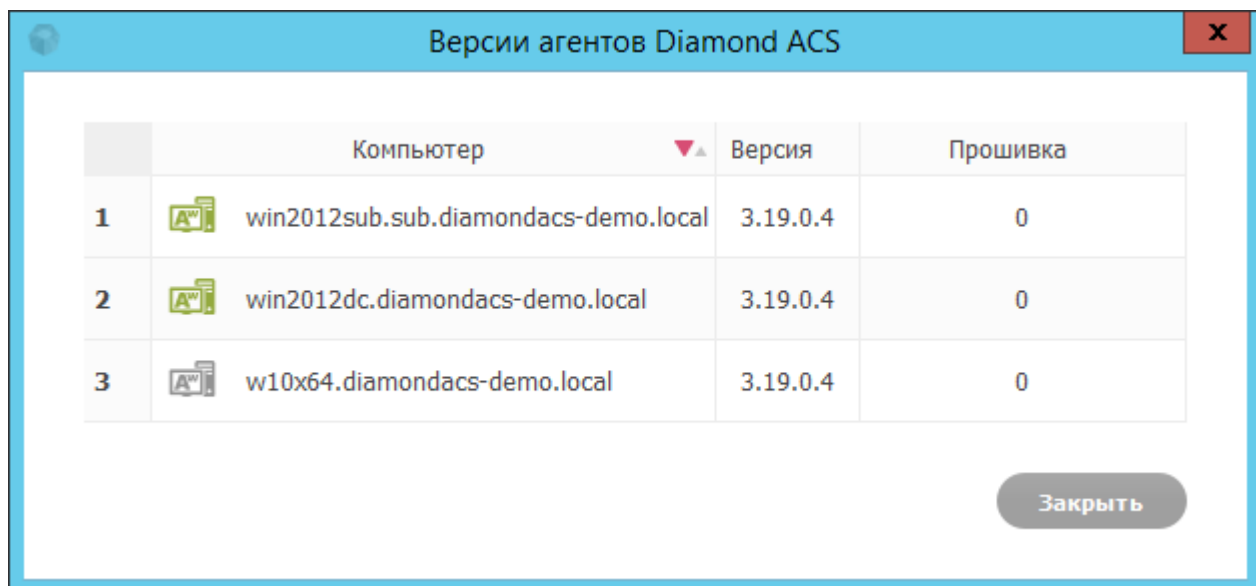


Рисунок 46 – Окно контроля версий установленных агентов на клиентских компьютерах

Таблица 10 – Описание окна контроля версий установленных агентов.

Компьютер	Сетевое имя АРМ
Версия	Версия установленного агента безопасности на АРМ



Прошивка	Версия микропрограммы платы «Diamond ACS HW»
-----------------	----------------------------------------------

6.4 Контекстное меню действий над АРМ

Контекстное меню действий над АРМ изображено на рисунке 47. Описание контекстного меню действий над АРМ отображено в таблице 11.

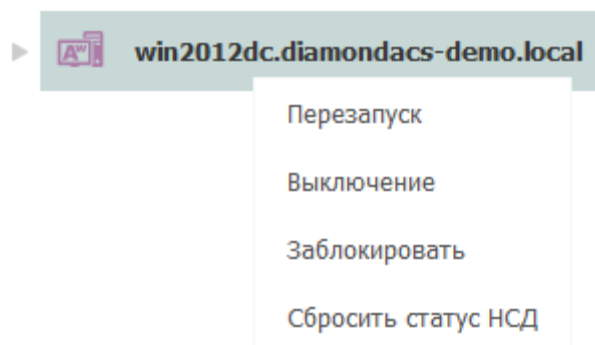


Рисунок 47 – Контекстное меню действий над АРМ

Таблица 11 – Описание контекстного меню действий над АРМ.

Перезапуск	Перезапуск клиентского АРМ
Выключение	Выключение клиентского АРМ
Заблокировать	Блокировка клиентского АРМ
Сбросить статус НСД	Сброс статуса НСД

6.5 Информационная панель

6.5.1 Просмотр общей информации

Для просмотра общей информации об АРМ необходимо выполнить следующие действия:

1. Нажать левой кнопкой мыши на иконке требуемого АРМ в окне «Иерархия».
2. В информационной панели выбрать вкладку «Информация» (см. рисунок 48).



Нулевые значения программных версий означают, что информация об установленной версии приложения «Diamond ACS Agent Workstation Net» отсутствует, так как данное АРМ не устанавливало соединения с сервером. Нулевое значение версии ПО аппаратного модуля «Diamond ACS HW» может свидетельствовать об отсутствии данного модуля на АРМ. Описание вкладки «Информация» отображена в таблице 12.



Рисунок 48 – Вкладка «Информация», отображающая основные свойства выбранного АРМ

Таблица 12 – Описание вкладки «Информация».

SID	Идентификатор безопасности
Имя	Сетевое имя АРМ
IP	IP-адрес АРМ
Статус	Текущее состояние АРМ
Последняя активность	Время последней активности на АРМ
Количество НСД	Количество НСД на АРМ



Версия	Версия установленного агента безопасности на АРМ
Версия прошивки	Версия микропрограммы платы Diamond ACS HW
ОС	Название операционной системы, установленной на АРМ
Версия ОС	Номер версии операционной системы, установленной на АРМ
Пакет обновления ОС	Версия пакета обновления операционной системы, установленной на АРМ

6.5.2 Контроль целостности данных

Для просмотра нарушений правил контроля целостности необходимо выполнить следующие действия:

1. Нажать левой кнопкой мыши на иконке требуемого АРМ в окне «Иерархия».
2. В информационной панели выбрать вкладку «Контроль целостности» (см. рисунок 49).

Если ранее, во время текущего подключения «Diamond ACS Security Monitor», для выбранного в иерархии АРМ не выполнялось других действий, касающихся контроля целостности, то во вкладке контроля целостности будут присутствовать только те объекты, целостность которых была нарушена. Описание вкладки «Контроль целостности» отображено в таблице 13.

Получение полного списка объектов, для которых задан контроль целостности, инициируется нажатием кнопки «Перечитать» на панели фильтрации в нижней правой части окна.

Для объектов, целостность которых была нарушена, поле «CRC» выделено красным жирным шрифтом.

Критерии нарушения целостности ресурса:

- изменение данных – в поле хеша будет новое значение;



СКРД Diamond ACS. Инструкция по настройке и эксплуатации

- отсутствие указанного ресурса (при удалении, переименовании, перемещении и др.) – вместо хеша будет указано, что объект удален или больше не находится под контролем целостности.

Для принятия изменений объектов необходимо:

1. Выбрать требуемый объект или несколько объектов.
2. Нажать кнопку «Принять» на панели фильтрации.

В случае принятия изменений список объектов меняется следующим образом:

- при изменении данных – выделение поля «CRC» снимается;
- при отсутствии указанного ресурса – запись об объекте удаляется из списка контроля целостности.

win2012dc.diamondacs-demo.local

Информация **Контроль целостности** Diamond ACS Приложение Система Безопасность

	Имя	CRC	Время
1	C:\Program Files\Diamond Security\Diamond ACS\Client\DmADDTs.dll	1e697b16617ab8ae38b8696336becb6e	23.03.2016 18:07:03.363
2	C:\Program Files\Diamond Security\Diamond ACS\Client\DmADSI.dll	2e0b352c8b43684cc1378e44e219a6e6	23.03.2016 18:07:03.440
3	C:\Program Files\Diamond Security\Diamond ACS\Client\DmAgent.dmp	14179d887243eac77f0d84b3cccb4da4	27.04.2016 18:00:03.593
4	C:\Program Files\Diamond Security\Diamond ACS\Client\DmAgent.exe	08684cb1ed9988828d2e4668dd498a8d	23.03.2016 18:07:03.457
5	C:\Program Files\Diamond Security\Diamond ACS\Client\DmCredentialProvider.dll	1ba7febf4bae3d2329a6e924b23d59dd	12.05.2016 13:19:24.640
6	C:\Program Files\Diamond Security\Diamond ACS\Client\DmCredentialProvider.dll_	- удален или снят с контроля	12.05.2016 13:19:24.687
7	C:\Program Files\Diamond Security\Diamond ACS\Client\DmCSL.dll	e777c81958d4fb5dbfc6b248f1bacd55	23.03.2016 18:07:03.473
8	C:\Program Files\Diamond Security\Diamond ACS\Client\DmDCL.dll	457186e03881a0aa856ea5819401e189	23.03.2016 18:07:03.473
9	C:\Program Files\Diamond Security\Diamond ACS\Client\DmNTDIL.dll	8ebb5ac5f5fd52f20f03c934db3ebd82	23.03.2016 18:07:03.473
10	C:\Program Files\Diamond Security\Diamond ACS\Client\DmPCL.dll	f80e4f6201a06c61647efcc7c08e9c21	23.03.2016 18:07:03.473
11	C:\Program Files\Diamond Security\Diamond ACS\Client\DmPCL.exe	a74e30a071b5f9c60a7da8920e7c6798	23.03.2016 18:07:03.597

Дата/время: с 12.05.2016 0:00 по 12.05.2016 16:32

Синхронизовать Перечитать Принять

Рисунок 49 – Вкладка «Контроль целостности» приложения «Diamond ACS Monitor»

Таблица 13 – Описание вкладки «Контроль целостности».

Имя	Контролируемый объект
CRC	Контрольная сумма
Время	Время снятие контрольной суммы



6.5.3 Просмотр журналов

Для просмотра журналов «Diamond ACS», «Приложение», «Система», «Безопасность» необходимо выполнить следующие действия:

1. Нажать левой кнопкой мыши на иконке требуемого АРМ в окне «Иерархия».
2. В информационной панели выбрать соответствующую вкладку (см. рисунок 50).

По умолчанию при выборе в иерархии некоторого АРМ, для каждого из журналов запрашиваются только те события, которые произошли за текущие сутки. Для запроса любой другой части журнала или всего журнала, необходимо выбрать соответствующую вкладку и указать желаемый период времени, затем нажать кнопку обновления информации «Перечитать».

Сервер автоматически собирает журналы с АРМ при их подключении, а затем с периодичностью в 1 час. Поэтому при запросе журнала с помощью кнопки «Перечитать» будет получена только та информация, которая хранится в данный момент на сервере безопасности. Для получения актуальных данных необходимо дать серверу безопасности команду запроса журнала с клиента, нажав кнопку «Синхронизировать». При установленном флаге «Очищать после выгрузки» в настройках АРМ в момент нажатия кнопки «Синхронизировать» выбранный журнал будет очищен на АРМ. В случае получения сообщения «Ошибка 0x80070005: Отказано в доступе» при попытке синхронизации необходимо в «Diamond ACS Manager» в настройках АРМ включить выгрузку данного журнала. Описание вкладки «Diamond ACS» отображено в таблице 14.

Тип	Сообщение	Дата/время	Событие	Источник	Категория	Пользователь	Компьютер	Данные
Information	Иницирование отправки журнала событий на сервер безопасности Тип журнала: diamond Код ошибки: 0x00000000 Описание: Операция успешно завершена.	13.05.2016 15:29:42.000	204	DmAgentService	Администрирование		win2012dc.diamondacs-demo.local	
Error	Несанкционированный доступ пользователя к файлу	13.05.2016 15:29:22.000	100	DmAgentService	Контроль доступа		win2012dc.diamondacs-demo.local	
Information	Создание процесса Windows	13.05.2016 15:24:41.000	213	DmAgentService	Аудит доступа к ресурсам		win2012dc.diamondacs-demo.local	
Information	Создание процесса Windows	13.05.2016 15:24:13.000	213	DmAgentService	Аудит доступа к ресурсам		win2012dc.diamondacs-demo.local	
Information	Создание процесса Windows	13.05.2016 15:24:13.000	213	DmAgentService	Аудит доступа к ресурсам		win2012dc.diamondacs-demo.local	
Information	Модификация реестра Windows	13.05.2016 15:24:11.000	212	DmAgentService	Аудит доступа к ресурсам		win2012dc.diamondacs-demo.local	
Information	Модификация реестра Windows	13.05.2016 15:24:11.000	212	DmAgentService	Аудит доступа к ресурсам		win2012dc.diamondacs-demo.local	
Information	Создание процесса Windows	13.05.2016 15:24:10.000	213	DmAgentService	Аудит доступа к ресурсам		win2012dc.diamondacs-demo.local	
Information	Создание процесса Windows	13.05.2016 15:24:10.000	213	DmAgentService	Аудит доступа к ресурсам		win2012dc.diamondacs-demo.local	
Information	Модификация реестра Windows	13.05.2016 15:23:56.000	212	DmAgentService	Аудит доступа к ресурсам		win2012dc.diamondacs-demo.local	
Information	Модификация реестра Windows	13.05.2016 15:23:56.000	212	DmAgentService	Аудит доступа к ресурсам		win2012dc.diamondacs-demo.local	

Рисунок 50 – Отображение журнала «Diamond ACS»



Таблица 14 – Описание вкладки «Diamond ACS».

Тип	Тип произошедшего события
Сообщение	Общее описание события
Дата/время	Дата и время события
Событие	Идентификатор события
Источник	Источник события
Категория	Категория события
Пользователь	???
Компьютер	Полное имя компьютера, на котором произошло событие
Данные	???

6.6 Информация о сервере безопасности

6.6.1 Просмотр информации

Для просмотра информации о сервере безопасности необходимо выполнить следующие действия:

1. Выбрать требуемый сервер безопасности в окне «Иерархия».
2. В информационной панели выбрать вкладку Информация.

Вкладка «Информация» отображает основные свойства компьютера с установленным сервером безопасности «Diamond ACS Server» (см. рисунок 51). Описание вкладки «Информация» отображено в таблице 15.



SID	S-1-5-21-2950390329-1598033167-3156007200-1001
Имя	win2012dc.diamondacs-demo.local
IP	172.20.1.115/255.255.255.0
Статус	работает
Последняя активность	11.05.2016 14:41:33.811
Версия	3.19.0.4
ОС	Windows Server 2012 R2 Standard (x64)
Версия ОС	6.3 (9600)
Пакет обновления ОС	

Рисунок 51 – Вкладка «Информация»

Таблица 15 – Описание вкладки «Информация».

SID	Идентификатор безопасности
Имя	Сетевое имя
IP	IP-адрес
Статус	Текущее состояние
Последняя активность	Время последней активности
Версия	Версия установленного сервера безопасности



ОС	Название операционной системы
Версия ОС	Номер версии операционной системы
Пакет обновления ОС	Версия пакета обновления операционной системы

6.6.2 Просмотр сессий

Для просмотра информации о сервере безопасности необходимо выполнить следующие действия:

1. Выбрать требуемый сервер безопасности в окне «Иерархия».
2. В информационной панели выбрать вкладку «Сессии» (см. рисунок 52).

При подключении к серверу безопасности приложений СКРД «Diamond ACS» на сервере с каждым из них открывается сессия. В рамках данной сессии производится запись действий, производимых в отношении сервера. Такими действиями могут быть инициирование и завершение загрузки журнала с клиентского АРМ, отправка команд на блокировку/перезагрузку/выключение АРМ и другие события со стороны подключившегося приложения.

Поле выбора «Действия» позволяет фильтровать действия, отображая в правой части вкладки «Сессии» только те из них, которые произошли в рамках выбранных сессий (по умолчанию после загрузки журнала отображаются все действия). Сами действия описываются текстовым полем «Действие» правой части вкладки и содержат всю необходимую информацию о произошедшем событии. Кроме того, указаны время и код результата события.



win2012dc.diamondacs-demo.local

Информация Сессии

Действия	Приложение	Компьютер	Пользователь	IP	Начало	Окончание	Код завершения	Действие	Дата/время	Код завершения	
1	Агент	DIAMONDACS-DEMO\...	DIAMONDACS-DEMO\WIN201...	172.20.1.115	13.05.2016 1...	-	-	1	Инициирование процед...	13.05.2016 16:14:0...	0
2	Монитор	DIAMONDACS-DEMO\...	DIAMONDACS-DEMO\Админи...	172.20.1.115	13.05.2016 1...	-	-	2	Получен запрос от мон...	13.05.2016 16:02:2...	0x80070005
3	Монитор	DIAMONDACS-DEMO\...	DIAMONDACS-DEMO\Админи...	172.20.1.115	13.05.2016 1...	13.05.2016 16...	0	3	Получен запрос от мон...	13.05.2016 16:02:2...	0
4	Монитор	DIAMONDACS-DEMO\...	DIAMONDACS-DEMO\Админи...	172.20.1.115	12.05.2016 1...	13.05.2016 15...	0	4	Завершение операции ...	13.05.2016 16:02:0...	0
5	Конфигуратор на...	DIAMONDACS-DEMO\...	DIAMONDACS-DEMO\Админи...	172.20.1.115	12.05.2016 1...	-	-	5	Инициирование операц...	13.05.2016 16:02:0...	0
6	Сервер безопасн...	SUB\WIN2012SUB	SUB\WIN2012SUB\$	172.20.1.118	11.05.2016 1...	-	-	6	Завершение операции ...	13.05.2016 16:02:0...	0
7	Агент	DIAMONDACS-DEMO\...	DIAMONDACS-DEMO\WIN201...	172.20.1.115	11.05.2016 1...	13.05.2016 16...	0	7	Инициирование операц...	13.05.2016 16:02:0...	0
8	Собственный сер...	DIAMONDACS-DEMO\...	DIAMONDACS-DEMO\WIN201...	127.0.0.1	11.05.2016 1...	-	-	8	Завершение операции ...	13.05.2016 16:02:0...	0
9	Собственный сер...	DIAMONDACS-DEMO\...	DIAMONDACS-DEMO\WIN201...	127.0.0.1	11.05.2016 1...	-	-	9	Инициирование операц...	13.05.2016 16:02:0...	0
10	Собственный сер...	DIAMONDACS-DEMO\...	DIAMONDACS-DEMO\WIN201...	127.0.0.1	11.05.2016 1...	-	-	10	Попытка открытия сесс...	13.05.2016 16:01:4...	0
11	Сервер безопасн...	SUB\WIN2012SUB	SUB\WIN2012SUB\$	172.20.1.118	29.04.2016 1...	-	-	11	Завершение операции ...	13.05.2016 16:01:3...	0
12	Собственный сер...	DIAMONDACS-DEMO\...	DIAMONDACS-DEMO\WIN201...	127.0.0.1	29.04.2016 1...	-	-	12	Завершение процедуры...	13.05.2016 16:00:5...	0
13	Собственный сер...	DIAMONDACS-DEMO\...	DIAMONDACS-DEMO\WIN201...	127.0.0.1	29.04.2016 1...	-	-	13	Получен запрос от мон...	13.05.2016 16:00:4...	0x800700aa
14	Собственный сер...	DIAMONDACS-DEMO\...	DIAMONDACS-DEMO\WIN201...	127.0.0.1	29.04.2016 1...	-	-	14	Получен запрос от мон...	13.05.2016 16:00:4...	0
15	Сервер безопасн...	SUB\WIN2012SUB	SUB\WIN2012SUB\$	172.20.1.118	28.04.2016 1...	-	-	15	Инициирование процед...	13.05.2016 16:00:4...	0
16	Собственный сер...	DIAMONDACS-DEMO\...	DIAMONDACS-DEMO\WIN201...	127.0.0.1	28.04.2016 1...	-	-				

Дата/время: с 13.05.2016 0:00 по 13.05.2016 16:14

Сохранить Прочитать Печать

Рисунок 52 – Вкладка «Сессии»



7 Типовые ошибки и способы их устранения

AD Assistant не удается смодифицировать схему AD. Ошибка – «Схема AD занята».	Причина ошибки – нарушена репликация между контроллерами домена. Необходимо устранить данную причину.
Установка модуля DmAgent.msi заканчивается действием «Rollback».	Для устранения проблемы необходимо: 1. Убедиться, что защищаемое АРМ включено в домен. 2. Убедиться, что процесс установки осуществляется доменным пользователем. 3. Если защищаемая ОС автоматически обновляется, перезагрузить АРМ. 4. Проверить АРМ на наличие вирусов.
Установка модуля DmServer.msi заканчивается действием «Rollback».	Для устранения проблемы необходимо: 1. Убедиться, что сервер СКРД «Diamond ACS» включен в защищаемый домен. 2. Убедиться, что версия AD обновлена до нужной для работы СКРД «Diamond ACS». 3. Убедиться, что правильно указываете путь до базы данных «Microsoft SQL Server» или «PostgreSQL». 4. Убедиться, что правильно указываете имя и пароль администратора домена. 5. Убедиться, что правильно указываете имя экземпляра «Microsoft SQL Server».



	<p>б. Убедиться, что для учетной записи «NT Authority\Система» в настройках SQL Server «Безопасность->Имена входа» установлен флаг system для роли сервера.</p>
<p>DmAgent.msi не устанавливается. В логах – Нет доступа к реестру (Access is denied).</p>	<p>Для устранения проблемы необходимо отключить службу «Удаленный реестр».</p>
<p>На ОС XP x86 не устанавливается DmAgent. В логе ошибка: 126 (The specified module could not be found) при установке драйвера виртуального принтера (VPrinterInstallDriver).</p>	<p>Для устранения проблемы необходимо скопировать файлы srclient.dll, framedyn.dll из Windows\system32\DllCache в windows\system32.</p>
<p>При попытке аутентификации в Diamond ACS Security Manager или Security Monitor появляется сообщение об ошибке: «Для вызываемой службы действует лицензия на определенное число подключений...».</p>	<p>СКРД «Diamond ACS» не активирован или нет достаточного количества лицензий на удаленное подключение.</p> <p>Необходимо подключиться к серверу безопасности локально (используя localhost или 127.0.0.1) и выполнить активацию (см. см. п. 4).</p>
<p>Не удается подключиться к серверу безопасности с помощью «Security Monitor»</p>	<p>Проверить, что на компьютере с установленным сервером безопасности в межсетевом экране есть правило, разрешающее входящие подключения по TCP-порту, указанному в настройке «Слушающий порт» сервера безопасности (по умолчанию TCP-порт 8030).</p>



	<p>Убедиться, что на сервере безопасности запущена и работает служба «Diamond ACS Server» (нет ошибок в журналах).</p>
<p>При установке DmAgent.msi или DmServer.msi возникает ошибка:</p> <p>«There is a problem with this Windows Installer package. A DLL required for this install to complete could not be run. Contact your support personnel or package vendor»</p>	<p>Необходимо загрузить и установить распространяемый пакет Microsoft Visual C++ 2008 соответствующей битности операционной системе.</p> <p>Для 32-битной версии:</p> <p>https://www.microsoft.com/ru-ru/download/details.aspx?id=29</p> <p>Для 64-битной версии:</p> <p>https://www.microsoft.com/ru-ru/download/details.aspx?id=15336</p>



8 Глоссарий

Информация – это любые сведения вне зависимости от формы их представления.

Доступ к информации – возможность получения информации и ее использования.

Защита информации – совокупность методов и средств, обеспечивающих целостность, конфиденциальность, достоверность, аутентичность и доступность информации в условиях воздействия на нее угроз естественного или искусственного характера.

Контроль доступа – процесс защиты данных и программ от их использования объектами, не имеющими на это права.

Несанкционированный доступ – доступ к программам и данным, который получают абоненты, которые не прошли регистрацию и не имеют права на ознакомление или работу с этими ресурсами. Для предотвращения несанкционированного доступа осуществляется контроль доступа.

Автоматизированная система – комплекс технических, программных, других средств и персонала, предназначенный для автоматизации различных процессов.

Автоматизированное рабочее место – индивидуальный комплекс технических и программных средств, предназначенный для автоматизации профессионального труда специалиста и обеспечивающий подготовку, редактирование, поиск и выдачу на экран и печать необходимых ему документов и данных.

VPN – виртуальная частная сеть. Обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх любой сети вне зависимости от ее уровня доверия.

Токен – это компактное устройства в виде USB-брелока, которое служит для идентификации или авторизации пользователя. Также может выступать в роли хранилища сертификата электронно-цифровой подписи.

Смарт-карта – это компактное устройства в виде карты, которое служит для идентификации или авторизации пользователя. Также может выступать в роли хранилища сертификата электронно-цифровой подписи.