|  |  |  |
| --- | --- | --- |
|  |  | **УТВЕРЖДАЮ**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_…….. |
|  |  | ………  |
|  |  | «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2019 г. |

**Система криптографической защиты информации в базах данных**

**Подсистема криптографической защиты данных**

**Руководство пользователя «Крипто БД»**

**СОДЕРЖАНИЕ**

[**ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ** 3](#_Toc27731667)

[1. АННОТАЦИЯ 6](#_Toc27731668)

[2. СПИСОК СОКРАЩЕНИЙ 6](#_Toc27731669)

[3. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 7](#_Toc27731670)

[**4.** **ОБЩИЕ СВЕДЕНИЯ** 7](#_Toc27731671)

[4.1. Версия программного обеспечения Клиент "Крипто БД" 7](#_Toc27731672)

[4.2. Назначение комплекса 8](#_Toc27731673)

[4.3. Состав комплекса 8](#_Toc27731674)

[**4.4.** **Требования к квалификации персонала** 8](#_Toc27731675)

[**4.5.** **Алгоритмы и размеры ключей** 8](#_Toc27731676)

[**5.** **СИСТЕМНЫЕ ТРЕБОВАНИЯ** 8](#_Toc27731677)

[**5.1.** **Поддерживаемые СУБД и версии** 8](#_Toc27731678)

[**5.2.** **Дополнительная конфигурация программного обеспечения Oracle** 9](#_Toc27731679)

[**5.3.** **Программная конфигурация автоматизированного рабочего места пользователя** 9](#_Toc27731680)

[**5.4.** **Ключевые носители** 9](#_Toc27731681)

[**5.5.** **Инфраструктура открытых ключей** 9](#_Toc27731682)

[**6.** **ПОДГОТОВКА** 10](#_Toc27731683)

[**7.** **РЕКОМЕНДАЦИИ** 10](#_Toc27731684)

[**8.** **УСТАНОВКА И УДАЛЕНИЕ ПО Клиент "Крипто БД"** 10](#_Toc27731685)

[**8.1.** **Необходимые полномочия** 10](#_Toc27731686)

[**8.2.** **Локальные процедуры установки и удаления** 10](#_Toc27731687)

[**8.3.** **Централизованные процедуры установки и удаления** 14](#_Toc27731688)

[**8.4.** **Удалённые процедуры установки и удаления** 14](#_Toc27731689)

[**9.** **НАСТРОЙКА АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА** 16](#_Toc27731690)

[**10.** **ИСПОЛЬЗОВАНИЕ КЛИЕНТА "Крипто БД"** 16](#_Toc27731691)

[**11.** **ЛИТЕРАТУРА** 17](#_Toc27731692)

[**Предметный указатель** 18](#_Toc27731693)

**ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ**

| **Сокращение или обозначение** | **Расшифровка** |
| --- | --- |
| API | Application Programming Interface |
| FTP | File Transfer Protocol |
| HTTP | HyperText Transfer Protocol |
| HTTPS | HyperText Transfer Protocol Secure |
| NFS | Network File System |
| NGFW | Next generation firewall |
| RDP | Remote Desktop Protocol |
| SMB | Server Message Block |
| SMTP | Simple Mail Transfer Protocol |
| SSH | Secure Shell |
| SSL | Secure Sockets Layer |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| UDS | Universal Desktop Services |
| URL | Uniform Resource Locator |
| VDI | Virtual Desktop Infrastructure |
| VLAN | Virtual Local Area Network |
| АРМ | Автоматизированное рабочее место |
| АПК | Аппаратно-программный комплекс |
| БД | База данных |
| ВМ | Виртуальная машина |
| ГПБ | Групповая политика безопасности |
| Криптоферма | Комплекс аппаратно-программных средств для построения криптографических туннелей и объединенных в ферму для увеличения производительности |
| ЛВС | Локальная вычислительная сеть |
| ЛПБ | Локальная политика безопасности |
| НСД | Несанкционированный Доступ |
| ОС | Операционная система |
| ПАК | Программно-аппаратный комплекс |
| ПО | Программное обеспечение |
| РД | Руководящие документы |
| СУБД | Система управления базами данных |
| СХД | Система хранения данных |
| ФЗ | Федеральный закон |
| ФСТЭК России | Федеральная служба по техническому и экспортному контролю России |
| BIOS | Базовая система ввода-вывода (Base Input-Output System) |
| ITU-T | Международный комитет по телекоммуникациям (International Telecommunication Union)  |
| IETF | Специальная комиссия интернет разработок (Internet Engineering Task Force)  |
| АС  | Автоматизированная система  |
| АРМ  | Автоматизированное рабочее место  |
| БД | База данных |
| ДСЧ | Датчик случайных чисел |
| HDD, НЖМД | Накопитель на жёстких магнитных дисках |
| НСД  | Несанкционированный доступ  |
| ОС  | Операционная система  |
| ПАК  | Программно-аппаратный комплекс  |
| ПО  | Программное обеспечение  |
| ПЭВМ | Персональная электронная вычислительная машина |
| СВТ  | Средства вычислительной техники  |
| СКЗИ  | Средство криптографической защиты информации  |
| СОС (CRL) | Список отозванных сертификатов (Certificate Revocation List)  |
| СУБД | Система управления базой данных |
| УЦ | Удостоверяющий Центр |
| ЭЦП  | Электронная цифровая подпись  |
| ITU-T | Сектор стандартизации телекоммуникаций Международного комитета по телекоммуникациям (International Telecommunication Union Telecommunication [Standardization](http://en.wikipedia.org/wiki/Standardization) Sector)  |
| IETF | Специальная комиссия интернет разработок (Internet Engineering Task Force)  |
| АРМ  | автоматизированное рабочее место  |
| БД | база данных |
| ЗАО | закрытое акционерное общество |
| ПО  | программное обеспечение  |
| СУБД | система управления базой данных |
| УЦ | удостоверяющий центр |
| ЭЦП | электронная цифровая подпись |

# АННОТАЦИЯ

Настоящий документ содержит сведения, необходимые пользователю для установки и эксплуатации программно-аппаратного комплекса Клиент "Крипто БД".

# ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Администратор безопасности — субъект доступа, основной обязанностью которого является обеспечение конфиденциальности информации в базе данных, которую он курирует. Система административного управления безопасностью включает в себя комплекс организационно-технических мер, направленных на обеспечение конфиденциальности информации.

Аутентификация — проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Закрытый ключ — криптографический ключ, который хранится пользователем системы в тайне.

Открытый ключ — криптографический ключ, который связан с закрытым ключом с помощью особого математического соотношения. Открытый ключ известен другим пользователям системы.

Пароль — Секретная информация аутентификации, обычно представляющая собой строку знаков, которой должен обладать пользователь для доступа к защищённым данным.

Сертификат открытого ключа — структурированная двоичная запись в формате ASN.1, состоящая из:

* имени субъекта или объекта системы, однозначно идентифицирующего его в системе;
* открытого ключа субъекта или объекта системы;
* дополнительных атрибутов, определяемых требованиями использования сертификата в системе;
* ЭЦП издателя (УЦ), заверяющей совокупность этих данных.

Формат сертификата определён в рекомендациях ITU-T 1997 года X.509 [X.509] и рекомендациях IETF 1999 года RFC 2459 [PKIX]. В настоящее время основным принятым форматом является формат версии 3, позволяющий определить расширения (extensions), с помощью которых реализуется определённая политика безопасности в системе.

Удостоверяющий центр — центр управления открытыми ключами в соответствии с рекомендациями X509 в части использования сертификатов открытых ключей.

1. **ОБЩИЕ СВЕДЕНИЯ**

## Версия программного обеспечения Клиент "Крипто БД"

Текущая версия ПО Клиент "Крипто БД" — 2.0.

## Назначение комплекса

Клиент "Крипто БД" — программно-аппаратный комплекс, осуществляющий аутентификацию в СУБД на основе сертификатов открытого ключа, хранящихся в памяти USB-ключей и смарт-карт, а также для работы с СКЗИ "Крипто БД". Сведения, представленные далее, относятся к функциональности, обеспечивающей задачи аутентификации в СУБД. Сведения об использовании для работы с СКЗИ "Крипто БД" приведены в документе "RU.46538383.50 1430 005-01 92 01. Крипто БД. Руководство администратора безопасности. Часть I".

## Состав комплекса

В состав комплекса входят ПО Клиент "Крипто БД" и USB-ключи и/или смарт-карты с записанными в их память лицензиями на использование комплекса Клиент "Крипто БД".

**Примечание**

Если у вас есть ключи без лицензии на использование комплекса Клиент "Крипто БД", вы можете приобрести лицензии у ближайшего дилера ЗАО «Аладдин Р. Д.».

* 1. **Требования к квалификации персонала**

Внедрение комплекса Клиент "Крипто БД" и управление им должны осуществляться квалифицированными администраторами БД, обладающими навыками администрирования инфраструктуры открытого ключа и корпоративной редакции СУБД Oracle.

* 1. **Алгоритмы и размеры ключей**

Алгоритм генерации открытого и закрытого ключа — RSA. Допустимые размеры открытого ключа — 512, 1024 и 2048 бит.

1. **СИСТЕМНЫЕ ТРЕБОВАНИЯ**
	1. **Поддерживаемые СУБД и версии**

Клиент "Крипто БД" предназначен для работы со следующими редакциями сервера БД Oracle:

* Oracle Database Server 9i release 2 Enterprise Edition;
* Oracle Database Server 10g Enterprise/Standard/Standard Edition One;
* Oracle Database Server 11g Enterprise/Standard/Standard Edition One;
* Oracle Database Server 12c Enterprise/Standard/Standard Edition One.

Требования к ОС сервера БД Oracle не предъявляются.

* 1. **Дополнительная конфигурация программного обеспечения Oracle**

Для обеспечения возможности аутентификации пользователей в СУБД по протоколу SSL требуется дополнительная настройка как на стороне сервера БД, так и на стороне клиента. Инструкции по настройке SSL-аутентификации для поддерживаемых версий ПО Oracle приведены в [12], [13], [14], [15], [16].

* 1. **Программная конфигурация автоматизированного рабочего места пользователя**

На АРМ пользователя требуется предварительная установка всех программных продуктов, указанных в Табл. 1.

Табл. 1 — Основные программные компоненты АРМ пользователя

|  |  |
| --- | --- |
| **Разработчик** | **Наименование ПО** |
| Microsoft | Windows 7/8.1/10 (x86/x86-64)  |
| Oracle | Oracle Client 9i, 10g,11g или 12с for Windows XP/Vista/7/8/8.1 x86-64 |

* 1. **Ключевые носители**

В качестве носителей закрытых ключей могут выступать устройства следующих типов:

* смарт-карта или USB-токен JaCarta;
* реестр Windows;
* файлы, формата .p12.
	1. **Инфраструктура открытых ключей**

Для получения сертификатов пользователей вам потребуются услуги УЦ, издавшего сертификат для экземпляра сервера базы данных. Этот УЦ должен быть способен издавать сертификаты с ключами RSA для субъекта, наименование которого соответствует внешнему или глобальному имени пользователя Oracle. Определяемая в сертификате политика применения закрытого ключа (**Key Usage**) должна включать **Client Authentication**.

В действующей инфраструктуре открытого ключа должно быть установлено доверие к сертификатам, издаваемым данным УЦ. В частности, на рабочей станции пользователя корневой центр сертификации должен входить в число доверенных корневых центров сертификации локального компьютера, а сертификаты всех промежуточных центров сертификации должны присутствовать в хранилище сертификатов промежуточных центров сертификации локального компьютера.

1. **ПОДГОТОВКА**

Изданный с соблюдением условий, указанных в подразделе 5.5 настоящего документа, сертификат импортируется вместе с соответствующим ему закрытым ключом в персональный с лицензией Клиент "Крипто БД". Подготовленный таким образом передаётся пользователю с соблюдением принятых в организации регламентов.

1. **РЕКОМЕНДАЦИИ**

Для АРМ, на которых устанавливается Клиент "Крипто БД", рекомендуется:

* использование ПО в строгом соответствии с лицензиями фирм-разработчиков;
* отсутствие у установленного ПО средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам;
* проверка на наличие аппаратных закладок;
* проверка на отсутствие вирусов и программных закладок;
* исключение возможности несанкционированного изменения аппаратной части (опечатывание системных блоков, разъёмов и контроль печатей администратором безопасности);
* контроль целостности установленного ПО и его окружения после завершения процесса установки.
1. **УСТАНОВКА И УДАЛЕНИЕ ПО Клиент "Крипто БД"**
	1. **Необходимые полномочия**

Для установки Клиент "Крипто БД" на АРМ пользователя необходимы полномочия локального администратора данного АРМ.

* 1. **Локальные процедуры установки и удаления**
		1. **Локальная установка программного обеспечения Клиент "Крипто БД" на автоматизированное рабочее место пользователя**
			1. **Язык интерфейса программы установки**

Язык интерфейса программы установки Клиент "Крипто БД" определяется автоматически по языку интерфейса операционной системы.

* + - 1. **Установка ПО Клиент "Крипто БД" на автоматизированное рабочее место пользователя**

Локальная установка ПО Клиент "Крипто БД" на АРМ пользователя проводится штатным ПО установки. Для того чтобы установить ПО Клиент "Крипто БД" на АРМ пользователя, выполните следующую последовательность действий:

* Проверьте АРМ на соответствие требованиям к программной конфигурации и рекомендациям, приведённым в разделе 34.2. При необходимости приведите АРМ в соответствие указанным требованиям и рекомендациям.
* С компакт-диска Клиент "Крипто БД" запустите файл SLOra.msi.
* В открывшемся окне с условиями использования ПО ЗАО «Аладдин Р.Д.» (рис. 1) прочтите лицензионное соглашение. Если для этого вам потребуется его напечатать, нажмите **Печать**.
* Если вы не согласны с условиями лицензионного соглашения, нажмите **Отмена**. В этом случае ПО Клиент "Крипто БД" не будет установлено.
* Установите флажок **Я принимаю условия лицензионного соглашения** и нажмите **Установить**.

Рис. 1 — Установка ПО Клиент "Крипто БД" на АРМ пользователя. Начало установки

* Установка займёт некоторое время, по прошествии которого появится окно завершения процесса установки (рис. 2). В этом окне нажмите **Готово**.

Рис. 2 — Установка ПО Клиент "Крипто БД" на АРМ пользователя. Завершение установки

* + 1. **Локальное удаление программного обеспечения Клиент "Крипто БД" с автоматизированного рабочего места пользователя**
			1. **Необходимые полномочия**

Для удаления Клиент "Крипто БД" с АРМ пользователей необходимы полномочия локального администратора данного АРМ.

* + - 1. **Процедура локального удаления программного обеспечения Клиент "Крипто БД" с автоматизированного рабочего места пользователя**

Локальное удаление Клиент "Крипто БД" с АРМ пользователя проводится штатными средствами. Для того чтобы ими воспользоваться, выполните следующее:

* С компакт-диска Клиент "Крипто БД" запустите файл SLOra.msi.

**Примечание**

Для отказа от удаления и завершения программы установки на любом шаге, кроме последнего, можно нажать **Отмена** и подтвердить завершение программы установки.

* В открывшемся окне мастера установки нажмите **Продолжить.**

**Примечание**

На любом шаге программы установки, кроме первого и последнего для возврата к предыдущему шагу можно нажать **Назад**.

* В изменения, исправления или удаления установленных компонентов нажмите **Удалить** (рис. 3).

Рис. 3 — Удаление Клиент "Крипто БД" с АРМ пользователя

* В окне подтверждения (рис. 4) нажмите Удалить.

Рис. 4 — Удаление Клиент "Крипто БД" с АРМ пользователя. Подтверждение удаления

* В окне завершения (рис. 5) нажмите Готово.

 Рис. 5 — Удаление Клиент "Крипто БД" с АРМ пользователя. Завершение удаления

* 1. **Централизованные процедуры установки и удаления**

В домене Windows 2000/Server 2003/2008 ПО Клиент "Крипто БД" можно устанавливать и удалять с помощью групповой политики. Подробно о настройке групповых политик для централизованной установки и удаления программного обеспечения см., например, в материалах [17], [18], [19].

При использовании Microsoft Windows Server 2003 или 2008 руководствуйтесь статьями базы знаний Microsoft [] или [] соответственно.

* 1. **Удалённые процедуры установки и удаления**

В сети Windows NT/2000/XP/7/Server 2003/2008 программы установки/удаления ПО Клиент "Крипто БД" могут быть запущены удалённо с помощью утилиты **PsExec**, входящей в пакет **PsTools**. При этом процедуры установка и удаления выполняются в автоматическом режиме без диалоговых окон. Пакет PsTools доступен для бесплатной загрузки на сайте Sysinternals (**http://www.sysinternals.com**).

Для запуска программы установки/удаления ПО Клиент "Крипто БД" на удалённом компьютере вам потребуются:

файл **SLOra.msi**;

файл **psexec.exe**, входящий в пакет **PsTools**.

Для того чтобы установить или удалить ПО Клиент "Крипто БД" на удалённом компьютере, выполните следующее.

* Нажмите **Пуск/Start > Выполнить/Run.**
* В окне **Запуск программы/Run** в поле **Открыть/Open** ведите:

**cmd**

* Нажмите **OK**.
* В окне **Командная строка**/**Command Prompt** для введите:
* для установки ПО Клиент "Крипто БД":

**<psexec> \\<computer> –s msiexec /qn /i <SLOra.msi>**

* для удаления ПО «SecurLogon для Oracle»:

**<psexec> \\<computer> –s msiexec /qn /x <SLOra.msi>**

где:

**<psexec>** — путь к файлу psexec.exe;

**<computer>** — имя удалённого компьютера;

**<SLOra.msi>** — сетевой путь к файлу SLOra.msi или локальный путь к этому файлу на удалённом компьютере;

* В случае успешного завершения удалённой процедуры в командной оболочке появится сообщение:

**msiexec exited on <computer> with error code 0,**

где **<computer>** — имя удалённого компьютера.

1. **НАСТРОЙКА АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА**

 Для того чтобы настроить АРМ пользователя на использование комплекса Клиент "Крипто БД", выполните следующую последовательность действий:

* Убедитесь в том, что рабочая станция удовлетворяют системным требованиям комплекса Клиент "Крипто БД", изложенным в разделе 5 настоящего документа. Если это не так, установите недостающее ПО.
* В папке, в которой установлено ПО Oracle Client for Windows 2000/XP/Vista/7/8/8.1 (ORACLE\_HOME) при необходимости отредактируйте содержимое файла **ORACLE\_HOME\network\admin\sqlnet.ora**:
	+ установите параметр **WALLET\_LOCATION** в **MCS**:

WALLET\_LOCATION =

(SOURCE =

(METHOD = MCS))

* При работе приложений, не позволяющих вводить пустые имя пользователя и/или пароль, в качестве имени пользователя вводится слово, определяемое компонентом **"Расширенный режим совместимости"**. По умолчанию - "**external**". Если вы хотите использовать другое слово, создайте в разделе реестра **HKEY\_LOCAL\_MACHINE\SOFTWARE\Aladdin\SLOra\Oracle** строковый параметр **OracleUser** и назначьте ему в качестве значения желаемое слово. Убедитесь также в том, что режим совместимости активен, т.е. параметр **CompatibilityMode** в разделе реестра **HKEY\_LOCAL\_MACHINE\SOFTWARE\Aladdin\SLOra\Oracle** принимает значение **1**.
1. **ИСПОЛЬЗОВАНИЕ КЛИЕНТА "Крипто БД"**

После выполнения всех описанных выше мероприятий пользователи, снабжённые подготовленными , могут осуществлять аутентификацию с помощью комплекса Клиент "Крипто БД" на настроенных АРМ. При этом должен использоваться тот сетевой псевдоним, который определяет соединение по протоколу SSL. с лицензией на использование комплекса Клиент "Крипто БД" должен быть подключён к компьютеру. Световой индикатор USB-ключа должен гореть.

Для большинства современных приложений вы можете использовать пустые имя пользователя и пароль. Однако в некоторых приложениях это невозможно. Для работы с такими приложениями в качестве имени пользователя вводите слово, определяемое компонентом "Расширенный режим совместимости" (по умолчанию это слово **external**), а в качестве пароля — произвольный непустой пароль.

При подключении к серверу базы данных на экране появляется окно выбора сертификата.

Для осуществления соединения выберите сертификат и нажмите **OK**, а затем введите PIN-код вашего .

**Примечание**

В случае, если в памяти установлен только один сертификат, окно выбора сертификата не отображается, и имеющийся сертификат выбирается автоматически.

1. **ЛИТЕРАТУРА**

1. [Oracle® Database Advanced Security Administrator's Guide 11g Release 2 (11.2). Part Number E10746-02](http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/toc.htm).

1. [Oracle® Database Advanced Security Administrator's Guide 11g Release 1 (11.1). Part Number B28530-03](http://download.oracle.com/docs/cd/B28359_01/network.111/b28530/toc.htm).

1. [Oracle® Database Advanced Security Administrator's Guide 10g Release 2 (10.2). Part Number B14268-02](http://download.oracle.com/docs/cd/B19306_01/network.102/b14268/toc.htm).

1. [Oracle® Database Advanced Security Administrator's Guide 10g Release 1 (10.1). Part Number B10772-01](http://download.oracle.com/docs/cd/B14117_01/network.101/b10772/toc.htm).

1. [Oracle Advanced Security Administrator's Guide Release 2 (9.2). Part Number A96573-01](http://download.oracle.com/docs/cd/B10501_01/network.920/a96573/toc.htm).
2. Microsoft Knowledge Base, Article 302430: HOW TO: Assign Software to a Specific Group By Using a Group Policy;
3. Microsoft Official Curriculum, Course 2154B: Implementing and Administering Microsoft Windows 2000 Directory Services, Module 9: Using Group Policy to Maintain Software;
4. Зубанов Ф., Microsoft Windows 2000. Планирование, развёртывание, установка, М., Русская редакция, 2000, с. 361.
5. Microsoft Knowledge Base, Article 324750: HOW TO: Assign Software to a Specific Group By Using a Group Policy in the Windows Server 2003 Family.
6. Microsoft Knowledge Base, Article 816102: HOW TO: Use Group Policy to remotely install software in Windows Server 2003 and in Windows Server 2008.

**Предметный указатель**

Client Authentication, 10

подготовка, 11, 17

лицензия, 9

назнчение, 9

применение, 17

Key Usage, 10

RSA, 9, 10

Windows

2000, 15, 61, 71

NT, 15, 61, 71

Server 2003, 15, 61, 71

Server 2008, 15, 61, 71

XP, 15, 61, 71

АРМ

настройка, 17

деинсталляция

удалённая, 15, 61, 71

централизованная, 15, 63, 72

доверие, 10

использование, 17

ключевые носители, 10

лицензия, 9, 15, 61, 71

настройка, 17

рекомендации, 11

сетевой псевдоним, 17

системные требования

требования к Oracle Client, 10

требования к Oracle Database, 9

требования к операционной системе, 10

удостоверяющий центр, 10

установка

удалённая, 15, 61, 71

централизованная, 15, 63, 72

центр сертификации

корневой, 10

промежуточный, 10