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

**Система криптографической защиты информации в базах данных**

**Подсистема криптографической защиты данных**

**Руководство администратора безопасности СКЗИ «Крипто БД»**

**СОДЕРЖАНИЕ**

[**ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ** 4](#_Toc28003486)

[1. АННОТАЦИЯ 7](#_Toc28003487)

[2. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 7](#_Toc28003488)

[3. ВЕРСИЯ СКЗИ "Крипто БД" 19](#_Toc28003489)

[4. НАЗНАЧЕНИЕ СКЗИ "Крипто БД 2.0" 19](#_Toc28003490)

[5. ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ И ХАРАКТЕРИСТИКИ СКЗИ "Крипто БД 2.0" 19](#_Toc28003491)

[5.1. Варианты исполнения 19](#_Toc28003492)

[5.2. Ограничение 20](#_Toc28003493)

[5.3. Среда функционирования 20](#_Toc28003494)

[5.4. Реализованные алгоритмы 23](#_Toc28003495)

[5.5. Ключевые носители 23](#_Toc28003496)

[5.6. Размеры ключей 24](#_Toc28003497)

[6. Состав СКЗИ "Крипто БД 2.0" 24](#_Toc28003498)

[7. Ключевая система. Общие положения 24](#_Toc28003499)

[7.1. Ключевые пары 24](#_Toc28003500)

[7.2. Сертификаты открытого ключа 25](#_Toc28003501)

[7.3. Ключи шифрования 25](#_Toc28003502)

[7.4. Сроки действия ключей 26](#_Toc28003503)

[8. Метки безопасности 26](#_Toc28003504)

[9. Задачи управления СКЗИ "Крипто БД 2.0" 27](#_Toc28003505)

[10. Общие сведения об управлении криптографическими ключами в СКЗИ "Крипто БД 2.0" 27](#_Toc28003506)

[10.1. Задачи, связанные с управлением криптографическими ключами 27](#_Toc28003507)

[10.2. Инструмент управления криптографическими ключами 28](#_Toc28003508)

[10.3. Инфраструктура криптографических ключей 28](#_Toc28003509)

[10.4. Управление ключами сервера 29](#_Toc28003510)

[10.5. Управление ключами шифрования 30](#_Toc28003511)

[10.6. Управление ключами шифрования пользователей 32](#_Toc28003512)

[10.7. Компрометация криптографических ключей 34](#_Toc28003513)

[10.8. Ведение журнала 35](#_Toc28003514)

[11. Контроль инфраструктуры 36](#_Toc28003515)

[12. Установка ПО СКЗИ "Крипто БД 2.0" 36](#_Toc28003516)

[12.1. Участники установки и порядок их действия 36](#_Toc28003517)

[12.2. Рекомендации 36](#_Toc28003518)

[12.3. Порядок установки 37](#_Toc28003519)

[12.4. Язык интерфейса программы установки 37](#_Toc28003520)

[12.5. Установка ПО "Крипто БД 2.0" на АРМ администратора безопасности 37](#_Toc28003521)

[12.6. Состав папки установки 43](#_Toc28003522)

[12.7. Установка объектов СКЗИ "Крипто БД 2.0" на сервере БД 44](#_Toc28003523)

[12.8. Установка ПО "Крипто БД 2.0" на АРМ пользователя 49](#_Toc28003524)

[13. Удаление ПО СКЗИ "Крипто БД 2.0" 51](#_Toc28003525)

[13.1. Участники удаления и порядок их действия 51](#_Toc28003526)

[13.2. Порядок удаления 51](#_Toc28003527)

[13.3. Удаление объектов "Крипто БД 2.0" с сервера 52](#_Toc28003528)

[13.4. Удаление ПО СКЗИ "Крипто БД 2.0" с АРМ администратора безопасности 54](#_Toc28003529)

[13.5. Удаление ПО СКЗИ "Крипто БД 2.0" с АРМ пользователей 56](#_Toc28003530)

[14. Использование консоли администратора безопасности 59](#_Toc28003531)

[14.1. Назначение консоли 59](#_Toc28003532)

[14.2. Условия использования консоли 60](#_Toc28003533)

[14.3. Соединение с целевой базой данных 60](#_Toc28003534)

[14.4. Управление ключами сервера БД 62](#_Toc28003535)

[14.5. Управление метками безопасности 67](#_Toc28003536)

[14.6. Управление ключами шифрования 68](#_Toc28003537)

[14.7. Шифрование данных 73](#_Toc28003538)

[14.8. Управление пользователями Крипто БД 92](#_Toc28003539)

[14.9. Управление ключами шифрования пользователей 95](#_Toc28003540)

[14.10. Управление сервером ключей 102](#_Toc28003541)

[14.11. Журнал служебных событий 105](#_Toc28003542)

[14.12. Контроль целостности 105](#_Toc28003543)

[15. Принципы защиты информации от НСД 106](#_Toc28003544)

[16. Обеспечение безопасности функционирования рабочих мест и серверов со встроенными средствами криптографической защиты 107](#_Toc28003545)

[17. Критерии качества паролей 111](#_Toc28003546)

[18. Нештатные ситуации при эксплуатации СКЗИ 112](#_Toc28003547)

[19. Литература 113](#_Toc28003548)

[Приложение А. Акт о готовности к работе 117](#_Toc28003549)

[Приложение Б. Пример журнала пользователей СКЗИ "Крипто БД 2.0" 119](#_Toc28003550)

[Приложение В. Перечень и обозначения алгоритмов шифрования 119](#_Toc28003551)

**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 |
| ИФНС | Инспекция ФНС Росии |
| 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 |

# АННОТАЦИЯ

Настоящий документ содержит сведения, необходимые администратору безопасности средства криптографической защиты информации (СКЗИ) "Крипто БД 2.0" для успешного выполнения своих функций.

# ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная информационная система — комплекс программных и технических средств, предназначенных для сбора, хранения, поиска и выдачи информации по запросам [12].

Автоматизированная система — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций [3].

Авторство информации — однозначное соответствие между содержанием и/или формой информации и субъектом (объектом), сформировавшим эту информацию. Для пользователя авторство полученной им из системы или канала связи информации означает однозначное установление источника, сформировавшего эту информацию (её автора).

Актуальность информации — свойство информации сохранять свои свойства (ценность) для субъекта (пользователя) в течение определённого периода времени.

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. Основные направления деятельности администратора безопасности:

* контроль целостности программного обеспечения;
* управление ключевой системой: хранение, ввод в действие, смена и уничтожение ключей шифрования, генерация закрытых и открытых ключей пользователей, используемых для защиты ключей шифрования;
* управление доступом пользователей системы к зашифрованным данным, управление аппаратными средствами хранения ключевой информации;
* зашифрование и расшифрование информации, хранящихся в таблицах базы данных;

Аутентификация — проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности [13].

Безопасность:

Состояние защищённости жизненно важных интересов личности, общества и государства от внутренних и внешних угроз [14].

Отсутствие недопустимого риска, связанного с возможностью нанесения ущерба [9].

Безопасность информации (информационная безопасность):

* Состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т. п. [15].
* Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз [13].

Блокирование информации — прекращение или затруднение доступа законных пользователей к информации [16].

Верификация:

* Установление соответствия принятой и переданной информации с помощью логических методов [17].
* Процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие [13].

Владелец информации:

* Субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации [11].
* Субъект информационных отношений, обладающий правом владения, распоряжения и пользованием информационным ресурсом по договору с собственником информации [18].

Государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации [19].

Документ — материальный объект с информацией, закреплённой созданным человеком способом для её передачи во времени и пространстве [10].

Документированная информация (документ) — зафиксированная на материальном носителе путём документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель [1].

Доступ к информации — возможность получения информации и её использования [1].

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

Зашифрование данных — процесс преобразования открытых данных в зашифрованные данные при помощи шифра.

Защита информации:

* Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [11].
* Комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, изменения, модификации (подделки), несанкционированного копирования, блокирования информации [15].

Защита информации от НСД — составная часть общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа. В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД, условно состоящей из следующих четырёх подсистем: управления доступом; регистрации и учёта; криптографической; обеспечения целостности [20].

Защищённое средство вычислительной техники (защищённая автоматизированная система) — средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты [13].

Идентификация — присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов [13].

Имитозащита — защита системы шифрованной связи от навязывания ложных данных [4].

Имитовставка — отрезок информации фиксированной длины, полученный по определённому правилу из открытых данных и ключа и добавленный к зашифрованным данным для обеспечения имитозащиты [4].

Информация — сведения (сообщения, данные) независимо от формы их представления [1].

Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств [1].

Ключ (криптографический ключ, ключ шифрования) — конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований [4].

Компрометация ключа — утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей, относятся следующие:

* Безвозвратная потеря ключевых носителей.
* Потеря ключевых носителей с их последующим обнаружением.
* Увольнение сотрудников, имевших доступ к ключевой информации.
* Нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа.
* Возникновение подозрений на утечку информации или её искажение в системе хранения данных.
* Нарушение печати на сейфе с ключевыми носителями.
* Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника)

Конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя [1].

Контроль доступа (управление доступом) — процесс ограничения доступа к ресурсам системы только разрешённым субъектам или объектам.

Криптографическая защита — защита данных при помощи криптографического преобразования данных [4].

Криптографическое преобразование — преобразование данных при помощи шифрования и (или) выработки имитовставки [4].

Лицензирование в области защиты информации — деятельность, заключающаяся в передаче или получении прав на проведение работ в области защиты информации [15].

Маскирующее значение — значение зашифрованного поля базы данных, подставляемое вместо его открытого значения и вместо соответствующего шифртекста при обращении к полю без применения ключа шифрования.

Мандатное управление доступом — разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности [13].

Мероприятия по защите информации — совокупность действий по разработке и/или практическому применению способов и средств защиты информации [11].

Метка безопасности — элемент ключа шифрования данных субъекта, который характеризует уровень доступа данного ключа.

Метка конфиденциальности — элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте [13].

Нарушитель безопасности информации — физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при её обработке техническими средствами [16].

Нарушитель правил разграничения доступа субъект доступа, осуществляющий несанкционированный доступ к информации [13].

Некорректный электронный документ — электронный документ, не прошедший процедуры расшифрования данных, а также документ, имеющий искажения в тексте сообщения (наличие и/или отсутствие символов, букв или цифр в расшифрованном (открытом) тексте документа, не позволяющее понять смысл электронного документа).

Непреднамеренное воздействие на информацию — ошибка пользователя, сбой технических и программных средств информационных систем, а также природное явление или иное нецеленаправленное на изменение информации воздействие, связанное с функционированием технических средств, систем или с деятельностью людей, приводящие к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации [11].

Несанкционированное воздействие на информацию — воздействие на защищаемую информацию с нарушением установленных прав и/или правил изменения информации, приводящее к искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации [11].

Несанкционированный доступ к информации (НСД):

* Получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации [11]
* Доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или автоматизированной системы (АС) [13] [21].

Носитель информации — физическое лицо или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин [11].

Обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам [1].

Объект доступа — единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа [13].

Объект защиты:

* Информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации [11].
* Информация, технические средства и технология её обработки, в отношении которых необходимо обеспечить безопасность информации [16].

Обработка информации — передача, приём, хранение, преобразование и отображение информации.

Организация защиты информации — содержание и порядок действий по обеспечению защиты информации [11].

Открытый ключ — криптографический ключ, который связан с закрытым ключом с помощью особого математического соотношения. Открытый ключ известен всем другим пользователям системы и предназначен для проверки электронной цифровой подписи, позволяет определить автора подписи и достоверность электронного документа, но не позволяет вычислить закрытый ключ.

Пароль:

* Идентификатор субъекта доступа, который является его (субъекта) секретом [13].
* Секретная информация аутентификации, обычно представляющая собой строку знаков, которой должен обладать пользователь для доступа к защищённым данным.

Персональные данные — любая информация, относящаяся к определённому или определяемому на основании такой информации физическому лицу (субъекту ПД), в том числе: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация [2].

Плановая смена ключей — смена ключей с установленной в системе периодичностью, не вызванная компрометацией ключей.

Пользователь (потребитель) информации — субъект, пользующийся информацией, полученной от её собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением [11].

Поставщик службы криптографии — ПО, реализованное как библиотека, динамически загружаемая в единое адресное пространство процесса, инициируемого прикладной задачей. Реализует функции шифрования, вычисления имитовставки, хэширования, генерации пользовательских ключей. Обеспечивает работу с сессионными ключами шифрования (генерация, экспорт/импорт в защищённом виде), закрытыми и открытыми ключами обмена, ввод ключей с ключевых носителей, защищённое хранение и уничтожение ключей в оперативной памяти.

Правило доступа к защищаемой информации — совокупность правил, регламентирующих порядок и условия доступа к защищаемой информации и её носителям [11].

Правила разграничения доступа (ПРД) — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа [13].

Разглашение информации — несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к этой информации [11].

Расшифрование данных — процесс преобразования зашифрованных данных в открытые данные при помощи шифра [4].

Регламентация — способ защиты информации в процессе функционирования системы мероприятий, создающих такие условия переработки защищаемых данных, при которых возможности несанкционированного доступа сводятся к минимуму. Считается, что для эффективной защиты необходимо строго регламентировать здания, помещения, размещение аппаратуры, организацию и обеспечение работы всего персонала, связанного с обработкой конфиденциальной информации [17].

Санкционированный доступ к информации — доступ к информации, не нарушающий правила разграничения доступа [13].

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

* имени субъекта или объекта системы, однозначно идентифицирующей его в системе;
* открытого ключа субъекта или объекта системы;
* дополнительных атрибутов, определяемых требованиями использования сертификата в системе;
* ЭЦП издателя (Удостоверяющего центра), заверяющую 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.

Собственник информации:

* Субъект информационных отношений, обладающий юридическим правом владения, распоряжения и пользования информационным ресурсом. Юридическое право владения, распоряжения и пользования информационным ресурсом принадлежит лицам, получившим этот информационный ресурс по наследству. Авторам открытий, изобретений, научно-технических разработок, рационализаторских предложений и т.д. принадлежит право владения, распоряжения и пользования информацией, источником которой они являются [18].
* Субъект, в полном объёме реализующий полномочия владения, пользования и распоряжения информацией в соответствии с законодательными актами [11].
* Юридическое или физическое лицо, владеющее информацией в соответствии с Законом о собственности [16].

Средства вычислительной техники — совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем [23].

Средство защиты от несанкционированного доступа — программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа [13].

Средство криптографической защиты информации — средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения её безопасности [13].

Субъект доступа — лицо или процесс, действия которого регламентируются правилами разграничения доступа [13].

Субъект информационных отношений — физическое или юридическое лицо, обладающее определённым правом по отношению к информационному ресурсу. В зависимости от уровня полномочий субъект информационных отношений может быть источником, собственником, владельцем или пользователем информации [18].

Техническое средство обработки информации — техническое средство, предназначенное для приёма, накопления, хранения, поиска, преобразования, отображения и передачи информации по каналам связи [15].

Угроза безопасности — совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства [14].

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

Уничтожение информации — действие, в результате которого информация перестает физически существовать в технических средствах ее обработки [16].

Управление ключами — создание (генерация) ключей, их хранение, распространение, удаление (уничтожение), учёт и применение в соответствии с политикой безопасности.

Утечка информации:

* Неконтролируемое распространение защищаемой информации в результате её разглашения, несанкционированного доступа к информации и получения защищаемой информации разведкой [11].
* Неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация доверена [17].

Функция хэширования — сопоставление произвольного набора данных в виде последовательности двоичных символов его образу фиксированной небольшой длины. Эта функция используется в процедурах электронной цифровой подписи для сокращения времени вычисления и проверки подписи. Эффект сокращения времени достигается за счёт вычисления подписи только под образом подписываемого набора данных [5].

Целевая база данных — база данных (экземпляр базы данных), содержащий информацию, защищённую или подлежащую защите с помощью шифрования.

Целостность информации:

* Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения) [13].
* Свойство информации, заключающееся в её существовании в неискажённом виде (неизменном по отношению к некоторому фиксированному её состоянию).

Шифр — совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определённым правилам с применением ключей [4].

Шифрование — взаимнооднозначное математическое (криптографическое) преобразование, зависящее от ключа, которое ставит в соответствие блоку открытой информации, представленной в некоторой цифровой кодировке, блок шифрованной информации, также представленной в цифровой кодировке. Термин "шифрование" объединяет в себе два процесса: зашифрование и расшифрование информации. Если зашифрование и расшифрование осуществляются с использованием одного и того же ключа, то такой алгоритм криптографического преобразования называется симметричным, в противном случае — асимметричным.

Шифровальные средства — средства криптографической защиты информации:

* реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для защиты информации (в том числе входящие в системы и комплексы защиты информации от несанкционированного доступа), циркулирующей в технических средствах, при её обработке, хранении и передаче по каналам связи, включая шифровальную технику;
* реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и электронной цифровой подписи;
* аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для изготовления и распределения ключевых документов, используемых в шифровальных средствах, независимо от вида носителя ключевой информации [15];
* ручные шифры, документы кодирования и другие носители ключевой информации.

Шифртекст — зашифрованные данные, результат зашифрования данных.

Электронная цифровая подпись — добавляемые к блоку данных данные, полученные в результате зависящего от закрытого ключа криптографического преобразования исходного блока данных, позволяющие приёмнику данных удостовериться в целостности блока данных и подлинности источника данных, а так же обеспечить защиту от подлога. Проверка электронной цифровой подписи под блоком открытой информации производится с помощью криптографического преобразования и открытого ключа, соответствующего закрытому ключу, участвовавшему в процессе вычисления ЭЦП. Электронная цифровая подпись обеспечивает целостность сообщений (документов), передаваемых по незащищенным телекоммуникационным каналам общего пользования в системах обработки информации различного назначения, с гарантированной идентификацией её автора (лица, подписавшего документ). Электронная цифровая подпись позволяет заменить при безбумажном документообороте традиционные печать и подпись. При вычислении цифровой подписи вместо обычной связи между печатью или рукописной подписью и листом бумаги выступает сложная математическая зависимость между электронным документом, закрытым и открытым ключами. Практическая невозможность подделки электронной цифровой подписи опирается на очень большой объем определённых математических вычислений. Подписание документа не меняет самого документа, оно только даёт возможность проверить подлинность и авторство полученной информации.

# ВЕРСИЯ СКЗИ "Крипто БД"

Текущая версия СКЗИ "Крипто БД" — 2.0.

# НАЗНАЧЕНИЕ СКЗИ "Крипто БД 2.0"

СКЗИ "Крипто БД 2.0" предназначено для обеспечения конфиденциальности и контроля целостности информации, хранящейся в таблицах баз данных целевой СУБД, посредством криптографического преобразования и имитозащиты в соответствии с [4] и [24].

# ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ И ХАРАКТЕРИСТИКИ СКЗИ "Крипто БД 2.0"

## Варианты исполнения

### Исполнение 1

СКЗИ "Крипто БД 2.0" в варианте исполнения 1 при условии выполнения требований, изложенных в разделе 15, относится к классу КС1, обеспечивая конфиденциальность информации от внешнего нарушителя, самостоятельно осуществляющего создание методов и средств реализации атак, а также самостоятельно реализующего атаки.

### Исполнение 2

СКЗИ "Крипто БД 2.0" в варианте исполнения 2 при условии выполнения требований, изложенных в разделе 15, относится к классу КС2, обеспечивая конфиденциальность информации от её нарушения внутренним нарушителем, не являющимся пользователем средств вычислительной техники, на которых реализованы СКЗИ и среда его функционирования, самостоятельно осуществляющим создание методов и средств реализации атак, а также самостоятельно реализующим атаки. Исполнение 2 требует дополнительной установки средств защиты от НСД (см. п. 5.3.5).

### Исполнение 3

СКЗИ "Крипто БД 2.0" в варианте исполнения 3 при условии выполнения требований, изложенных в разделе 15, относится к классу КС3, обеспечивая конфиденциальность информации от её нарушения внутренним нарушителем, являющимся пользователем средств вычислительной техники, на которых реализованы СКЗИ и среда его функционирования, самостоятельно осуществляющим создание методов и средств реализации атак, а также самостоятельно реализующим атаки. Исполнение 3 требует дополнительной установки средств защиты от НСД (см. п. 5.3.5).

## Ограничение

Средствами СКЗИ "Крипто БД 2.0" не допускается защищать информацию, составляющую государственную тайну.

## Среда функционирования

### Технические средства

Техническая архитектура СКЗИ "Крипто БД 2.0" предполагает установку ПО на следующих технических средствах:

* сервер БД;
* рабочая станция (АРМ) администратора безопасности на платформе x86-64;
* АРМ пользователей ИС, в которую входит СКЗИ "Крипто БД 2.0" на платформе x86-64.

### Требования к программной конфигурации сервера базы данных

#### Oracle

Компонент сервера СКЗИ "Крипто БД 2.0" функционирует под управлением:

* следующих версий сервера баз данных Oracle:
* Oracle Database Server 9i (Personal, Standard, Enterprise editions);
* Oracle Database Server 10g (Personal, Standard, Enterprise editions);
* Oracle Database Server 11g (Personal, Standard, Enterprise editions);
* Oracle Database Server 12c (Personal, Standard, Enterprise editions);
* следующих операционных систем:
* Linux (x86-64);
* IBM AIX 7;
* HP-UX PA-RISC;
* Solaris Operating System (x86-64);
* Solaris Operating System (64-bit SPARC).

#### Microsoft SQL Server

Компонент сервера СКЗИ "Крипто БД 2.0" функционирует под управлением следующих версий сервера баз данных:

* Microsoft SQL Server 2008/2008R2 (x64);
* Microsoft SQL Server 2012 (x64);
* Microsoft SQL Server 2014 (x64).

#### Tibero

* следующих версий сервера баз данных Tibero:
* Tibero Database Server v.5.x;
* Tibero Database Server v.6.x;
* следующих операционных систем:
* Linux (x86-64).

#### PostgreSQL

* следующих версий сервера баз данных PostgreSQL:
* PostgreSQL Server v.9.x;
* следующих операционных систем:
* Linux (x86-64).

### Требования к программной конфигурации АРМ администратора безопасности

На АРМ администратора безопасности требуется предварительная установка ПО, указанного в табл. 1.

Табл. 1 — Программная конфигурация АРМ администратора безопасности

|  |  |
| --- | --- |
| Разработчик | Наименование ПО |
| Microsoft | Windows 7/8/8.1 (x32/x64) |
| Microsoft | .NET Framework 4.0 или выше,  ODBC MSSQL Driver |
| Oracle | Oracle Client 9i, 10g,11g или 12c for Windows, или  Oracle Instant Client 10g/11g/12c for Windows |
| КриптоПро | СКЗИ КриптоПро 4.0 |

### Требования к программной конфигурации АРМ пользователя

На АРМ пользователя требуется предварительная установка всех программных продуктов, указанных в табл. 2, и одного из СКЗИ, перечисленных в табл. 3.

Табл. 2 — Основные программные компоненты АРМ пользователя

|  |  |
| --- | --- |
| Разработчик | Наименование ПО |
| Microsoft | Windows XP/Vista/7/8/8.1 (x32/x64),  .NET Framework 3.5 или выше,  ODBC MSSQL Driver |
| Oracle | Oracle Client 9i, 10g,11g или 12c for Windows, или  Oracle Instant Client 10g/11g/12c for Windows |
| Аладдин Р.Д. | Клиент Крипто БД версии 2.0 для соответствующей целевой СУБД |

Табл. 3 — Дополнительные СКЗИ, используемые на АРМ пользователей СКЗИ "Крипто БД 2.0" (для исполнений 1 и 2)

|  |  |
| --- | --- |
| Разработчик | Наименование СКЗИ |
| КриптоПро | КриптоПро 4.0 |

### Средства защиты от НСД

В исполнениях 2 и 3 на каждом АРМ администратора безопасности и пользователей используется одно из следующих средств защиты от НСД:

* программно-аппаратный комплекс "Аккорд-АМДЗ";
* электронный замок "Соболь".

## Реализованные алгоритмы

Алгоритмы шифрования ГОСТ28147-89 и ГОСТ Р 34.12-2015 реализованы в соответствии с [4], [24], [27], [28] в следующих режимах:

* режим простой замены (ECB);
* режим гаммирования (CTR);
* режим гаммирования с обратной связью (CFB).

Полный перечень возможных режимов приведён в Приложение В. Обозначения алгоритмов шифрования.

Примечание

Применение режима простой замены (ECB) **не рекомендуется** ввиду его низкой криптографической стойкости.

## Ключевые носители

В качестве носителей закрытых ключей могут выступать устройства, использование которых допускается сертифицированным СКЗИ, используемым на АРМ администратора безопасности или АРМ пользователей.

Состав считывателей и дополнительного ПО для них конкретизуется в зависимости от используемого сертифицированного СКЗИ и его исполнения.

Для автоматических процессов допускается хранение закрытых ключей в файлах, соответствующих требованиям ТК 026 "Парольная защита с использованием алгоритмов ГОСТ", ТК 026 "Транспортный ключевой контейнер", на жёстких дисках при условии распространения на HDD требований по обращению с ключевыми носителями, содержащихся в документации используемого сертифицированного СКЗИ.

Для варианта Исполнения 3 хранение закрытых ключей производится в файлах, соответствующих требованиям ТК 026 "Парольная защита с использованием алгоритмов ГОСТ", ТК 026 "Транспортный ключевой контейнер", на жёстких дисках при условии распространения на HDD требований по обращению с ключевыми носителями.

## Размеры ключей

Размеры ключей для защиты ключей шифрования в соответствии с [6],[25],[29]:

* закрытый ключ – 256 или 512 бит;
* открытый ключ - 512 бит.

Размеры ключей, используемых при симметричном шифровании — 256 бит.

# Состав СКЗИ "Крипто БД 2.0"

В состав ПО СКЗИ "Крипто БД 2.0" входят:

* ПО сервера БД:
* библиотеки, реализующие алгоритмы шифрования;
* библиотеки работы с ключами шифрования;
* сервис вычисления ключей шифрования;
* библиотеки работы с репозиторием;
* библиотеки контроля целостности;
* ПО АРМ администратора безопасности:
* программное обеспечение для конфигурации объектов базы данных (консоль администратора безопасности);
* сценарии для базы данных;
* ПО АРМ пользователя (клиент Крипто БД).

# Ключевая система. Общие положения

## Ключевые пары

Для сервера базы данных и для каждого пользователя, включая администраторов безопасности, создаётся по одной ключевой паре (открытый и закрытый ключи). Ключевые пары создаются с использованием сертифицированных СКЗИ (СКЗИ, которые можно использовать на АРМ администратора безопасности и пользователя указаны в подразделе 5.3). Ключевая пара для каждого пользователя сохраняется на персональном ключевом носителе (см. подраздел 5.5).

Примечание

Информация о формировании и хранении ключей сервера приведена в подразделе 10.4.

## Сертификаты открытого ключа

Принадлежность открытого ключа конкретному пользователю задаётся путём издания соответствующего [26] сертификата открытого ключа в каком-либо УЦ. При этом поле **Subject** (кому выдано) должно содержать уникальное имя пользователя, а определяемая в сертификате политика применения закрытого ключа (**Key Usage**) должна включать **Key Agreement** и/или **KeyEncipherement**. Сертификат также импортируется в персональный ключевой носитель, и ключевой носитель передаётся пользователю с соблюдением принятых в организации регламентов.

## Ключи шифрования

### Создание ключей шифрования

В СКЗИ "Крипто БД 2.0" ключ зашифрования логической единицы данных (колонки таблицы базы данных) совпадает с ключом расшифрования (симметричный ключ, далее "ключ шифрования"). Для операций шифрования информации в таблицах целевой базы данных СКЗИ "Крипто БД 2.0" может использовать произвольное количество ключей шифрования. Они создаются администратором безопасности с использованием сертифицированного СКЗИ (см. п. 5.3.3), преобразовываются согласно [6] и [25],[29] с использованием открытого ключа администратора безопасности и сохраняются в реестре OC Windows на АРМ администратора безопасности.

### Подготовка пользовательских копий ключей шифрования

Для предоставления пользователю доступа к какому-либо ключу шифрования и, следовательно, к данным, зашифрованным с помощью этого ключа, задействуется хранящийся в персональном ключевом носителе администратора безопасности закрытый ключ администратора безопасности и содержащийся в сертификате открытого ключа данного пользователя открытый ключ. Получающаяся в результате преобразованная согласно [6] и [25],[29] с помощью открытого ключа пользователя копия ключа шифрования (далее ключ шифрования пользователя) сохраняется в репозитории "Крипто БД 2.0".

### Использование ключей шифрования

Для обращения пользователя к зашифрованным данным производится следующая последовательность действий:

* Пользователь получает из репозитория "Крипто БД 2.0" защищённые с помощью своего открытого ключа ключи шифрования и открытый ключ сервера.
* С помощью хранящегося в персональном ключевом носителе закрытого ключа пользователь извлекает ключи шифрования и открытый ключ сервера.
* Пользователь преобразует извлечённые ключи шифрования согласно [6] и [25],[29] с использованием открытого ключа сервера и направляет их на сервер.
* На сервере полученные ключи шифрования извлекаются с помощью закрытого ключа сервера и далее используются для расшифрования защищённых данных в контексте сеанса пользователя.

Таким образом, для получения доступа к защищённым данным пользователю информационной системы необходимо иметь:

* персональный ключевой носитель с закрытым ключом;
* зашифрованные с использованием персонального открытого ключа копии ключей шифрования, хранящиеся в репозитории "Крипто БД 2.0".

Важно:

Администратор безопасности и пользователи системы должны принять меры для сохранения в тайне закрытых ключей, ключей шифрования, паролей (PIN-кодов) ключевых носителей, а также обеспечить сохранность самих ключевых носителей.

## Сроки действия ключей

Срок действия ключей сервера — 1 год 3 месяца.

Сроки действия закрытых и открытых ключей пользователей выбираются согласно рекомендациям производителей сертифицированных СКЗИ (см. подраздел 5.3).

Срок действия ключей шифрования — 1 год 3 месяца.

# Метки безопасности

Для дополнительного ограничения доступа к зашифрованным данным в СКЗИ "Крипто БД 2.0" реализован мандатный метод управления доступом. Метка представляет собой значение, характеризующее степень конфиденциальности информации. В качестве метки безопасности объекта выступает метка, содержащаяся в зашифрованном фрагменте данных (метка конфиденциальности). Метка субъекта входит в состав копии ключа шифрования пользователя. При обработке защищённых данных ПО "Крипто БД 2.0" сравнивает метки объекта и субъекта и принимает решение о зашифровании или расшифровании. Расшифрование возможно, если метка субъекта не меньше метки объекта. Зашифрование возможно, если метка субъекта не больше метки объекта.

# Задачи управления СКЗИ "Крипто БД 2.0"

Управление СКЗИ осуществляется администратором безопасности совместно с администраторами баз данных, администраторами сети и сводится к следующим задачам:

* установка и удаление СКЗИ "Крипто БД 2.0" (см. разделы 12 и 13);
* подготовка СКЗИ "Крипто БД 2.0" к эксплуатации (см. подраздел 14.10);
* управление криптографическими ключами (см. раздел 10);
* зашифрование и расшифрование данных (см. раздел 14.7);
* контроль инфраструктуры (см. раздел 11);
* учёт установленного ПО;
* ведение журналов (см. подраздел 10.8).

# Общие сведения об управлении криптографическими ключами в СКЗИ "Крипто БД 2.0"

## Задачи, связанные с управлением криптографическими ключами

Управление ключами шифрования, используемыми для защиты информации, хранящейся в таблицах БД, осуществляется администратором безопасности. В задачи администратора безопасности входят:

* контроль инфраструктуры управления криптографическими ключами;
* создание (генерация), смена и удаление ключей сервера;
* создание (генерация), смена и удаление ключей шифрования;
* создание и уничтожение ключей шифрования пользователей;
* резервное копирование и восстановление ключей шифрования;
* мониторинг нештатных ситуаций при работе с ключами шифрования и реакция на такие события;
* ведение журналов и разбор конфликтных ситуаций.

## Инструмент управления криптографическими ключами

Действия по управлению криптографическими ключами осуществляются с помощью консоли администратора, являющейся программным средством, входящим в состав СКЗИ "Крипто БД 2.0". Использование консоли администратора безопасности подробно описано в разделе 14 настоящего документа.

## Инфраструктура криптографических ключей

### Элементы инфраструктуры криптографических ключей

В состав инфраструктуры, управляющей криптографическими ключами, входят:

* хранилище ключей шифрования;
* удостоверяющий центр (УЦ);
* консоль администратора безопасности.

### Хранилище ключей шифрования

В качестве хранилища ключей шифрования используются следующие хранилища:

1. реестр ОС Windows на АРМ администратора безопасности для хранения ключей шифрования;
2. таблица базы данных, созданная в схеме администратора безопасности для хранения ключей шифрования пользователей (подробнее см. RU.46538383.50 1430 005-01 92 02. "Крипто БД. Руководство администратора базы данных Oracle", RU.46538383.50 1430 005-01 92 03. "Крипто БД. Руководство администратора базы данных MSSQL", RU.46538383.50 1430 005-01 92 04. "Крипто БД. Руководство администратора базы данных Tibero", RU.46538383.50 1430 005-01 92 05. "Крипто БД. Руководство администратора базы данных Postgres"). Данное хранилище содержит следующую информацию:

* идентификаторы пользователей;
* сертификаты пользователей;
* открытый ключ сервера БД, защищённый в соответствии с [6] и [25],[29] с применением открытых ключей пользователей;
* ключи шифрования, защищённые в соответствии с [6] и [25] ,[29] с применением открытых ключей пользователей;
* контрольная информация.

### Удостоверяющий центр

Удостоверяющий центр используется для управления закрытыми ключами и сертификатами пользователей, которые применяются для защиты ключей шифрования (см. подраздел 7.2). В качестве УЦ рекомендуется использовать УЦ, сертифицированный ФСБ, например, Удостоверяющий центр "КриптоПро УЦ" [ЖТЯИ.00009-01 30 01. Удостоверяющий центр "КриптоПро УЦ". Формуляр.].

Примечание

Для целей тестирования допускается использование центра сертификации корпорации Microsoft (Microsoft Certification Authority) или других удостоверяющих центров, соответствующих подразделу 7.2 настоящего документа либо утилита, входящая в состав ПО "Крипто БД 2.0" (см. раздел 7 документа "Руководство администратора безопасности. Часть II").

## Управление ключами сервера

### Формирование ключей сервера

Формирование ключей сервера (экземпляра базы данных) производится администратором безопасности следующим образом:

* администратор безопасности производит формирование закрытого и открытого ключа сервера (см. подраздел 14.4);
* закрытый и открытый ключи сервера, преобразованные согласно [6] и [25],[29] с использованием открытого ключа администратора безопасности, сохраняются на АРМ администратора безопасности;
* факт изготовления ключей сервера заносится в журнал пользователей "Крипто БД 2.0" и заверяется администратором безопасности.

### Копирование ключей сервера

При необходимости создаются копии открытого ключа сервера и защищённого паролем закрытого ключа сервера (например, при сменной работе нескольких администраторов безопасности и/или в целях резервного копирования). О создании каждой копии делается запись в журнале пользователей "Крипто БД 2.0".

Важно:

Рекомендуется не перезапускать программное обеспечение сервера ключей без необходимости.

## Управление ключами шифрования

### Задачи управления ключами шифрования

Задачи управления ключами шифрования выполняются администратором безопасности со своего АРМ с использованием консоли администратора безопасности (см. подраздел 14.5). К таким задачам относятся:

* создание (генерация) ключей шифрования;
* смена ключей шифрования (плановая и внеплановая);
* удаление ключей шифрования.

### Создание ключей шифрования

Общая схема, используемая для создания ключей шифрования, состоит из следующих этапов:

* анализ степени важности данных, для шифрования которых создаётся ключ;
* выбор алгоритма;
* генерация ключа;
* создание защищённой паролем резервной копии ключа шифрования и её сохранение;
* регистрация события создания ключа шифрования в журнале пользователей "Крипто БД 2.0".

### Смена ключей шифрования

Смена ключей шифрования может быть плановой и внеплановой. Плановая смена ключей шифрования происходит при истечении срока его действия, указанного в подразделе 7.4. Внеплановая смена ключей шифрования предусматривается для случаев их компрометации (см. п. 10.7.2).

Смена ключей шифрования происходит в следующем порядке:

* Администратор безопасности производит смену ключей согласно инструкциям, приведённым в п. 14.6.2.
* Для новых ключей шифрования создаются резервные копии, защищённые паролем. Эти копии хранятся у администратора безопасности.
* За21пись о событии смены ключа шифрования вносится в журнал пользователей "Крипто БД 2.0".

### Удаление ключей шифрования

Ключи шифрования, которыми не зашифрованы данные и которые не предполагается использовать для шифрования, должны быть удалены с помощью консоли администратора безопасности (см. п. 14.6.3). Также следует удалить все резервные копии удалённых ключей. Запись о событии удаления ключей шифрования вносится в журнал пользователей "Крипто БД 2.0".

## Управление ключами шифрования пользователей

### Инструмент для управления пользовательскими копиями ключей шифрования

Формирование и удаление ключей шифрования пользователей производится администратором безопасности с помощью консоли администратора безопасности (см. подраздел 13).

### Формирование ключей шифрования пользователя

Ключи шифрования пользователей создаются на основании приказа, заверенного подписью руководителя отдела информационной безопасности организации и печатью. Идентификаторы необходимых ключей шифрования должны быть перечислены в приказе. Пользователям в установленном порядке должны быть назначены аппаратные хранилища с закрытым ключом и сертификатом. Сертификаты пользователей предварительно передаются администратору безопасности.

Процедура создания ключей пользователя проходит следующим образом:

* Администратор безопасности на основании предоставленных документов создаёт ключи шифрования пользователя.
* Событие создания ключей шифрования пользователя заносится в журнал пользователей "Крипто БД 2.0".
* Администратор безопасности выдаёт пользователю карточку оповещения о компрометации, в которой указываются:
* телефоны отдела информационной безопасности;
* пароль (кодовое слово) администратора безопасности;
* уникальный пароль (кодовое слово) пользователя УЦ.

Примечание

Карточка оповещения применяется пользователями "Крипто БД 2.0" для сообщений о компрометации ключа по телефонным каналам общего пользования. Карточка оповещения должна храниться у пользователя наравне с ключами.

### Удаление ключей шифрования пользователей

Ключи шифрования пользователей удаляются в следующих случаях:

* на основании приказа, заверенного подписью руководителя отдела информационной безопасности организации и печатью;
* при получении оповещения о компрометации ключей пользователя.

Примечание

В случае, когда пользователь более не должен использовать "Крипто БД 2.0", если его закрытый ключ и сертификат были созданы исключительно для использования с "Крипто БД 2.0", они также уничтожаются. Если при этом аппаратный ключевой носитель использовался исключительно для применения с "Крипто БД 2.0", он форматируется.

Событие удаления ключей шифрования пользователя заносится в журнал "Крипто БД 2.0" для каждого пользователя.

## Компрометация криптографических ключей

### Общие сведения о компрометации криптографических ключей

Определение термина "компрометация", виды компрометации и основные события, приводящие к компрометации, приведены в разделе 2 "Основные термины и определения". По факту компрометации ключей должно быть проведено служебное расследование. Выведенные из действия скомпрометированные ключевые носители после проведения служебного расследования уничтожаются (форматируются), о чём делается запись в журнале пользователя "Крипто БД 2.0".

### Компрометация ключей шифрования

В случае компрометации ключа шифрования:

* должна быть остановлена работа сервера ключей (см. п. 14.10.2);
* сеансы пользователей, работающие с зашифрованными таблицами, должны быть принудительно завершены.
* работа пользователей и сервера ключей может быть восстановлена после внеочередной смены скомпрометированных ключей шифрования (см. п. 10.5.3).

### Компрометация закрытого ключа пользователя

#### Действия пользователя при компрометации его закрытого ключа

При компрометации закрытого ключа пользователя последний должен немедленно:

* прекратить работу с ПО, использующим СКЗИ "Крипто БД 2.0";
* известить администратора безопасности о компрометации ключа.

Информация о компрометации может передаваться по телефону с сообщением заранее условленного пароля, зарегистрированного в карточке оповещения о компрометации. После формирования новых ключевой пары и сертификата для пользователя создаётся новый набор ключей шифрования в установленном порядке.

#### Действия администратора безопасности в случае компрометации закрытого ключа пользователя

При получении сообщения о компрометации ключа одного из пользователей администратор безопасности:

* оповещает ответственное лицо УЦ о необходимости добавления сертификата, соответствующего скомпрометированному закрытому ключу, в список отозванных сертификатов (а УЦ при формировании очередного СОС включает в него отзываемый сертификат);
* удаляет копии ключей шифрования данного пользователя из репозитория "Крипто БД 2.0" (см. п. 14.9.5);
* после подтверждения со стороны ответственного лица УЦ о создании для пользователя нового закрытого ключа и сертификата, создаёт для пользователя новый набор ключей шифрования в соответствии со списком, полученным ранее при первичном создании копий ключей шифрования для данного пользователя.

## Ведение журнала

Администратор безопасности организации записывает в журнал пользователей "Крипто БД 2.0" факты создания и смены ключей шифрования, компрометации ключей, нештатные ситуации, происходящие в сети, проведение регламентных работ, данные о нештатных ситуациях, произошедших на АРМ и серверах баз данных с установленным ПО СКЗИ "Крипто БД 2.0".

В журнале пользователя "Крипто БД 2.0" должна отражаться следующая информация:

* дата;
* время;
* запись о создании, удалении, смене ключа шифрования, о зашифровании или расшифровании информации в таблице базы данных, о компрометации ключа, о создании ключей шифрования пользователей, либо о событиях, происходившие на АРМ пользователя или на серверах БД с установленным ПО СКЗИ, с указанием причин и предпринятых действий.

Примечание

Примерные графы журнала приведены в приложении Б.

# Контроль инфраструктуры

Задачи администратора безопасности по контролю инфраструктуры:

* регулярное резервное копирование репозитория "Крипто БД 2.0";
* периодический (не реже 1 раза в 2 недели) контроль целостности программного обеспечения и криптографических объектов "Крипто БД 2.0" на сервере СУБД;
* периодический (не реже 1 раза в 2 месяца) контроль программного окружения на АРМ администратора безопасности;
* периодический (не реже 1 раза в 2 месяца) контроль целостности ПО консоли администратора безопасности.

# Установка ПО СКЗИ "Крипто БД 2.0"

Примечание

Приведенные ниже снимки экрана процесса установки соответствуют целевой СУБД Oracle. Для других платформ шаги установки аналогичны, за исключением названия СУБД.

## Участники установки и порядок их действия

Порядок действий участников установки ПО СКЗИ "Крипто БД 2.0" описан в документеRU.46538383.50 1430 005-01 "Крипто БД. Описание реализации". В настоящем документе приводится подробное описание действий администратора безопасности, которые он должен выполнить после того как администратор БД выполнит свои действия.

## Рекомендации

К эксплуатации программного обеспечения, использующего СКЗИ "Крипто БД 2.0" допускаются лица, имеющие специальную подготовку и изучившие эксплуатационную документацию на соответствующие программные средства.

Для технические средств, на которых устанавливаются компоненты СКЗИ "Крипто БД 2.0" (см. п. 5.3.1), рекомендуется:

* использование ПО в строгом соответствии с лицензиями фирм-изготовителей;
* 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 серверов, рабочих станций (опечатывание серверного оборудования, системных блоков, разъёмов и контроль печатей администратором безопасности);
* обеспечение защиты каналов передачи данных между сервером базы данных с одной стороны и АРМ администратора безопасности и пользователей с другой стороны;
* проверка установленного ПО и его окружения после завершения процесса установки.

## Порядок установки

Установка СКЗИ должна выполняться в следующем порядке:

* установка ПО на АРМ администратора безопасности (см. подраздел 12.5);
* конфигурация объектов сервера БД (см. подраздел 12.7);
* установка ПО на рабочие станции пользователей (см. подраздел 12.8).

## Язык интерфейса программы установки

Язык интерфейса программы установки компонентов СКЗИ "Крипто БД 2.0" определяется автоматически по языку интерфейса операционной системы.

## Установка ПО "Крипто БД 2.0" на АРМ администратора безопасности

Установка ПО "Крипто БД 2.0" на АРМ администратора безопасности проводится штатным ПО установки, входящим в комплект поставки СКЗИ "Крипто БД 2.0". Для того чтобы установить ПО "Крипто БД 2.0" на АРМ администратора безопасности, выполните следующую последовательность действий:

* Проверьте АРМ на соответствие требованиям к программной конфигурации, приведённым в п. 5.3.3 и рекомендациям, приведённым в подразделе 12.2. При необходимости приведите АРМ в соответствие указанным требованиям и рекомендациям.
* С компакт-диска "Крипто БД 2.0" запустите файл:
* Aladdin.CryptoDB.Oracle.GOST.msi - для Oracle;
* Aladdin.CryptoDB.MSSQL.GOST.msi - для Microsoft SQL Server;
* Aladdin.CryptoDB.Postgres.GOST.msi - для PostgreSQL;
* Aladdin.CryptoDB.Tibero.GOST.msi - для Tibero.

Данный файл расположен в папках Win32 или x64 для версий OC Windows 32 или 64 bit соответственно.

* В открывшемся окне (рис. 1) нажмите Далее.

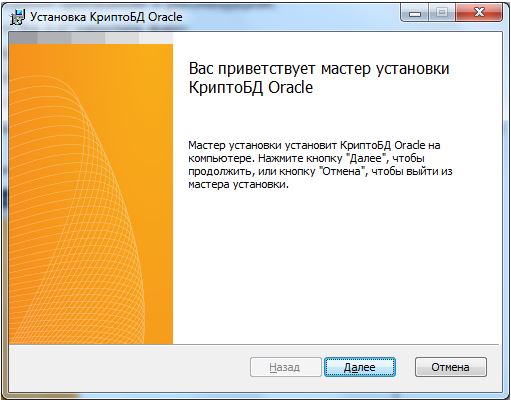


Рис. 1 — Установка ПО "Крипто БД 2.0" на АРМ администратора безопасности. Начало установки

* В открывшемся окне с условиями использования ПО "Аладдин Р.Д." (рис. 2) прочтите лицензионное соглашение. Если для этого вам потребуется его напечатать, нажмите Печать.
* Если вы не согласны с условиями лицензионного соглашения, нажмите Отмена и подтвердите завершение программы установки. В этом случае ПО "Крипто БД 2.0" не будет установлено.

Примечание

Отказаться от установки ПО "Крипто БД 2.0", нажав **Отмена** и подтвердив завершение программы установки, можно на любом её шаге, кроме последнего. Кроме того, на любом шаге, кроме последнего, можно вернуться на один шаг назад, нажав **Назад**.

* Установите флажок Я принимаю условия лицензионного соглашения и нажмите Далее.

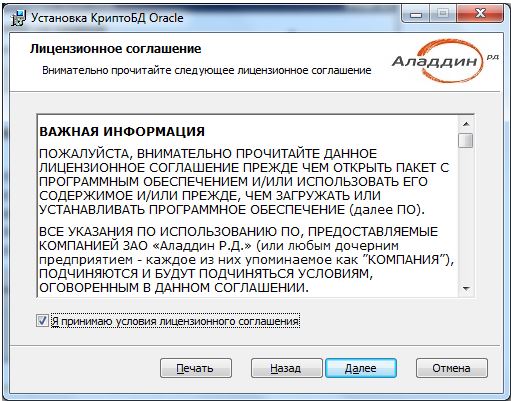


Рис. 2 — Установка ПО "Крипто БД 2.0" на АРМ администратора безопасности. Условия лицензионного соглашения

* В программе установки ПО "Крипто БД 2.0" предусмотрено три вида установки:
* обычная (устанавливаются все компоненты, кроме коллекторов аудита);
* выборочная (можно выбрать устанавливаемые компоненты вручную);
* полная (устанавливаются все компоненты).

В окне выбора типа установки нажмите **Обычная**, **Выборочная** или **Полная** (рис. 3).

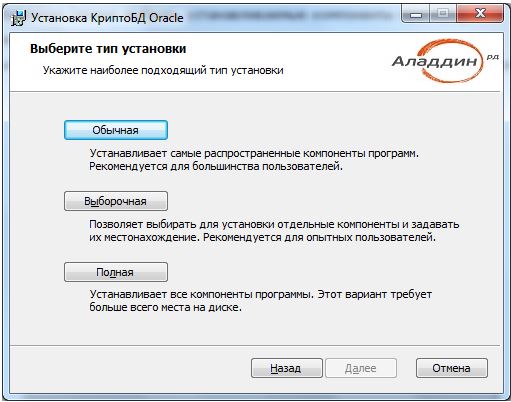


Рис. 3 — Установка ПО "Крипто БД 2.0" на АРМ администратора безопасности. Выбор типа установки

* Если вы выбрали обычную или полную установку, перейдите на шаг 10.
* Выберите компоненты, которые необходимо установить на АРМ администратора безопасности, настройте способ установки каждого из компонентов и нажмите Далее (рис. 4).

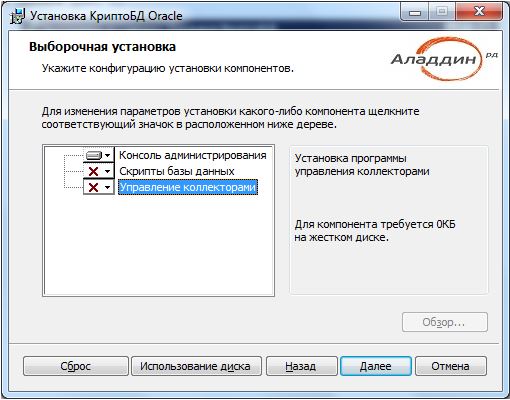


Рис. 4 — Установка ПО "Крипто БД 2.0" на АРМ администратора безопасности. Выбор компонентов

* В открывшемся окне выберите язык интерфейса устанавливаемого ПО в выпадающем списке и нажмите Далее (рис. 5).

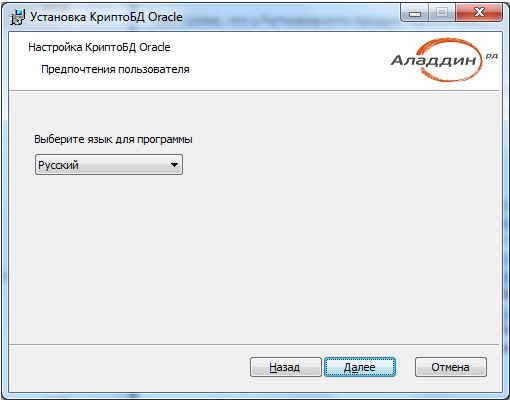


Рис. 5 — Установка ПО "Крипто БД 2.0" на АРМ администратора безопасности. Выбор языка интерфейса

* В открывшемся окне готовности к установке ПО "Крипто БД 2.0" нажмите Установить (рис. 6).

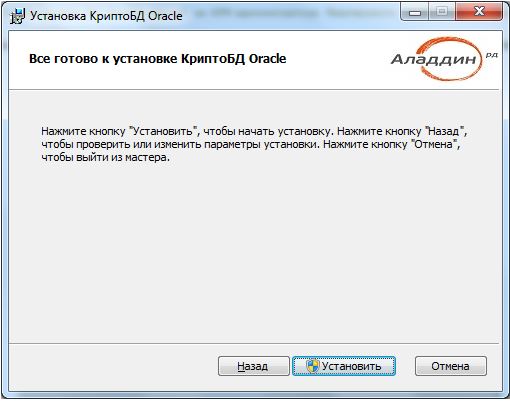


Рис. 6 — Установка ПО "Крипто БД 2.0" на АРМ администратора безопасности. Готовность к установке

* Установка займёт некоторое время, по прошествии которого появится окно завершения процесса установки (рис. 7). В этом окне нажмите Готово.

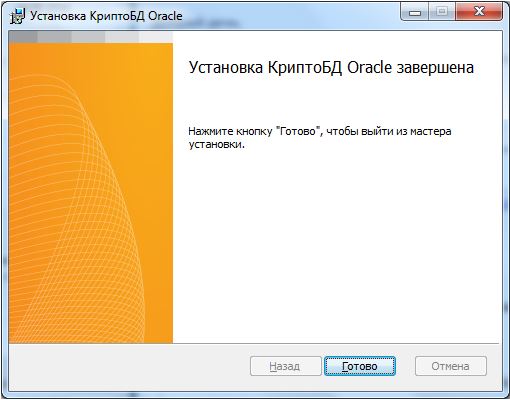


Рис. 7 — Установка ПО "Крипто БД 2.0" на АРМ администратора безопасности. Завершение установки

## Состав папки установки

ПО "Крипто БД 2.0" устанавливается в папку **"C:\Program Files\Aladdin\<DB>\CryptoDB\"**, где **<DB>** - целевая база данных.Помимо исполняемых модулей и библиотек, папка установки в зависимости от выбранного вида установки может содержать следующие предназначенные для администратора базы данных и администратора безопасности файлы (в подпапках):

* scripts\grantaccess.sql — сценарий назначения дополнительных прав пользователю - администратору безопасности для шифрования данных в таблицах;
* scripts\revokeaccess.sql — сценарий изъятия дополнительных прав у пользователя - администратора безопасности после завершения процедуры шифрования данных в таблицах;
* collector\collector.ini — шаблон конфигурации коллекторов аудита;
* collector\collector.jar — исполняемая библиотека коллектора аудита;
* collector\colStart.bat — сценарий запуска коллектора аудита (для ОС Windows);
* collector\colStop.bat — сценарий останова коллектора аудита (для ОС Windows);
* collector\\*.jar, \*.dll — служебные библиотеки для коллектора аудита;
* ru\\*.dll — служебные библиотеки.

Дополнительные файлы и утилиты располагаются в папке **"C:\Program Files\Aladdin\CAPI\<v.\*.\*>"**.

* Aladdin.CAPI.Store.exe - утилита управления ключевыми контейнерами (GUI);
* Aladdin.CAPI.Container.cmd - утилита управления ключевыми контейнерами (командная строка);
* \*.config - конфигурационные файлы;
* \*.dll — служебные библиотеки.

## Установка объектов СКЗИ "Крипто БД 2.0" на сервере БД

Установка объектов СКЗИ "Крипто БД 2.0" на сервере БД проводится штатной программой конфигурации (мастер конфигурации), которая запускается на АРМ администратора безопасности. Для того чтобы установить объекты СКЗИ "Крипто БД 2.0" на сервере БД, выполните следующую последовательность действий:

* Проверьте сервер БД на соответствие требованиям к программной конфигурации, приведённым в п. 5.3.2 и рекомендациям, приведённым в подразделе 12.2. При необходимости приведите сервер БД в соответствие указанным требованиям и рекомендациям.
* На АРМ администратора выберите в главном меню Windows Все программы -> Аладдин -> КриптоБД -> <Целевая БД> -> Конфигурирование КриптоБД (рис. 8).

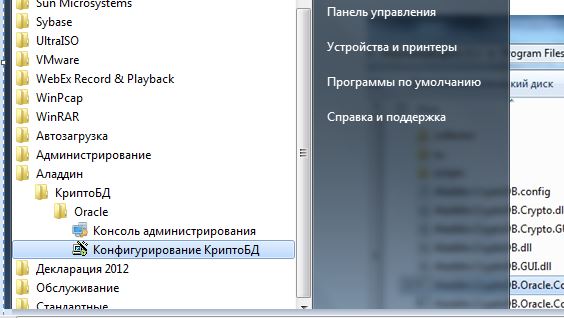


Рис. 8 — Запуск программы конфигурации серверных объектов СКЗИ "Крипто БД 2.0" (пример для Oracle)

* В открывшемся окне диалога (рис. 9) нажмите Далее.

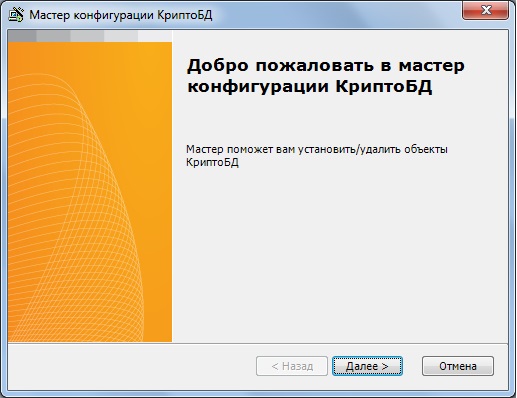


Рис. 9 — Начало конфигурации объектов СКЗИ "Крипто БД 2.0" на сервере

* В открывшемся окне (рис. 10) задайте имя службы целевой БД, имя системной учетной записи БД (администратора БД) и пароль для системной учётной записи целевой базы данных.

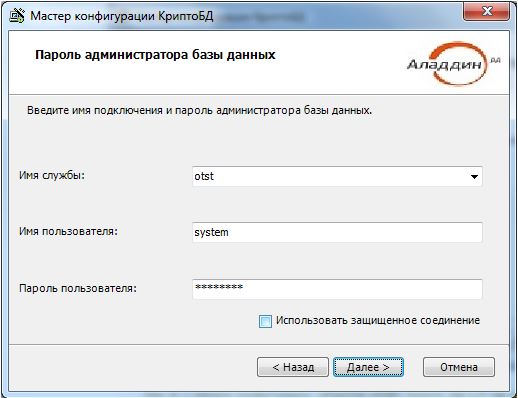


Рис. 10 — Программа конфигурации объектов СКЗИ "Крипто БД 2.0" на сервере. Ввод параметров подключения к базе данных (пример для Oracle)

* Для продолжения установки нажмите Далее.

Примечание

В качестве имени службы задаётся строка соединения с целевой БД. Описаниеформата строки связи и настройки сети для сервера БД приведено в документации по администрированию целевой СУБД соответствующей версии.

* Если вы готовы продолжить установку, в окне выбора режима конфигурации (рис. 11) выберите Установить объекты Крипто БД. Но если вы хотите исправить данные, введённые в предыдущем окне, нажмите Назад и вернитесь к шагу 4.

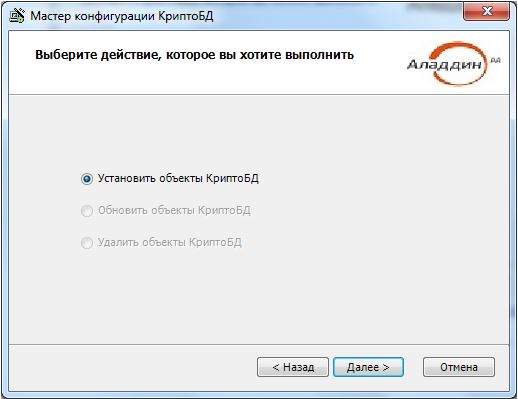


Рис. 11 — Установка объектов СКЗИ "Крипто БД 2.0" на сервере. Выбор действия

* Выберите ранее созданную схему пользователя целевой базы данных (схема владельца объектов, схема администратора безопасности) и укажите дополнительные параметры (например, табличное пространство для установки объектов схемы (рис. 12)).

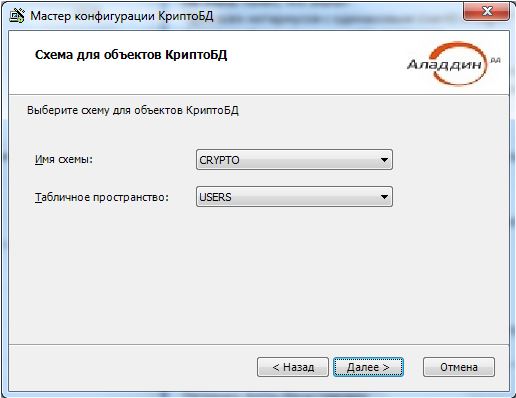


Рис. 12 — Установка объектов СКЗИ "Крипто БД 2.0" на сервере. Выбор схемы администратора безопасности (пример для Oracle)

Примечание

Требования к схеме владельца (администратора безопасности) и дополнительным параметрам приведены в документах для целевых СУБД:

* RU.46538383.50 1430 005-01 32 02 "Крипто БД. Руководство администратора базы данных Oracle";
* RU.46538383.50 1430 005-01 32 03 "Крипто БД. Руководство администратора базы данных MSSQL";
* RU.46538383.50 1430 005-01 32 04 "Крипто БД. Руководство администратора базы данных Tibero".
* Если вы хотите продолжить установку, нажмите Далее. Но если вы хотите исправить данные, введённые в предыдущем окне, нажмите Назад и вернитесь к шагу 8.
* Если вы хотите начать установку, в окне готовности к установке (рис. 13) нажмите Установить. Но если вы хотите исправить данные, введённые в предыдущем окне, нажмите Назад и вернитесь к шагу 8.

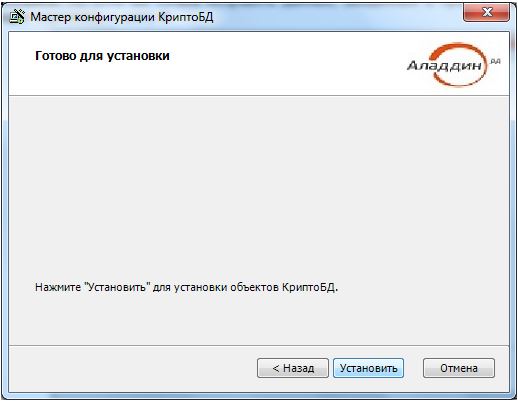


Рис. 13 — Установка объектов СКЗИ "Крипто БД 2.0" на сервере. Окно готовности к установке

* Установка займёт некоторое время, по прошествии которого появится окно завершения процесса установки (рис. 14). В этом окне нажмите Готово.

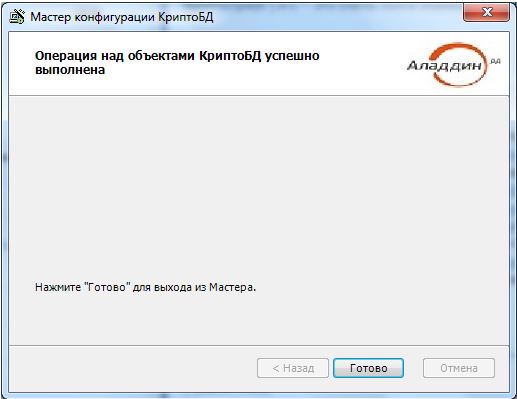


Рис. 14 — Установка объектов СКЗИ "Крипто БД 2.0" на сервере. Завершение работы мастера установки

## Установка ПО "Крипто БД 2.0" на АРМ пользователя

Установка ПО "Крипто БД 2.0" на АРМ пользователя проводится штатным ПО установки, входящим в комплект поставки СКЗИ "Крипто БД 2.0". Для того чтобы установить ПО "Крипто БД 2.0" на АРМ пользователя, выполните следующую последовательность действий:

* Проверьте АРМ на соответствие требованиям к программной конфигурации, приведённым в п. 5.3.4 и рекомендациям, приведённым в подразделе 12.2. При необходимости приведите АРМ в соответствие указанным требованиям и рекомендациям.
* С компакт-диска "Крипто БД 2.0" запустите файл (SLOra.msi - для Oracle, SLSql.msi - для MSSQL, SLTib.msi - для Tibero). Данный файл расположен в папках Win32 или x64 для версий OC Windows 32 или 64 bit соответственно.
* В открывшемся окне с условиями использования ПО "Аладдин Р.Д." (рис. 15) 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 "Крипто БД 2.0" не будет установлено.
* Установите флажок Я принимаю условия лицензионного соглашения и нажмите Установить.

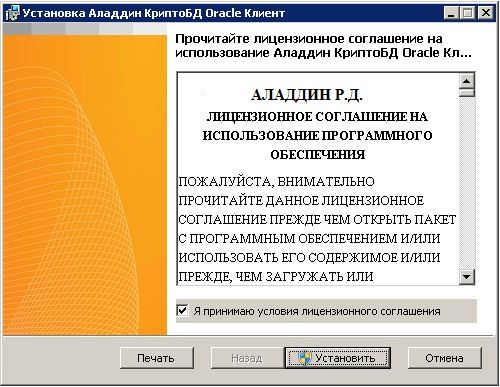


Рис. 15 — Установка ПО "Крипто БД 2.0" на АРМ пользователя. Начало установки (пример для Oracle)

* Установка займёт некоторое время, по прошествии которого появится окно завершения процесса установки (рис. 16). В этом окне нажмите Готово.

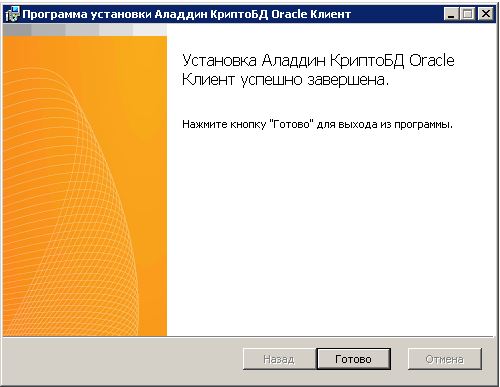


Рис. 16 — Установка ПО "Крипто БД 2.0" на АРМ пользователя. Завершение установки (пример для Oracle)

### Удалённые процедуры установки

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

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

* файл **SL<DB>.msi** (**SLOra.msi** - для Oracle, **SLSql.msi** - для MSSQL, **SLTib.msi** - для Tibero);
* утилита **psexec.exe**, входящий в пакет **PsTools**.

Для того чтобы установить ПО "Клиент Крипто БД" на удалённом компьютере, выполните следующие шаги:

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

**cmd**

1. Нажмите **OK**;
2. В окне **Командная строка/Command Prompt** для введите:

для установки ПО "Клиент Крипто БД":

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

где:

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

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

**<SL<DB>.msi>** — сетевой путь к файлу установки для соответствующей платформы БД или локальный путь к этому файлу на удалённом компьютере;

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

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

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

### Централизованные процедуры установки

В домене Windows ПО "Клиент Крипто БД" можно устанавливать и удалять с помощью групповой политики. Например, при использовании Microsoft Windows Server 2003 или 2008 руководствуйтесь статьями базы знаний Microsoft [33] или [34] соответственно.

# Удаление ПО СКЗИ "Крипто БД 2.0"

## Участники удаления и порядок их действия

Порядок действий участников удаления СКЗИ "Крипто БД 2.0" описан в документе RU.46538383.50 1430 005-01 "Крипто БД. Описание реализации". В настоящем документе приводится подробное описание действий администратора безопасности, которые он должен выполнить после того как администратор БД выполнит свои действия.

## Порядок удаления

Удаление ПО "Крипто БД 2.0" производится в следующем порядке:

* Удаление объектов "Крипто БД 2.0" с сервера БД.
* Удаление ПО с АРМ администратора безопасности.
* Удаление ПО с АРМ пользователей.

## Удаление объектов "Крипто БД 2.0" с сервера

Важно:

Удаление ПО Крипто БД с сервера базы данных уничтожает все ключи шифрования, сведения о таблицах с зашифрованными данными и очищает значение открытого ключа сервера в реестре рабочей станции администратора безопасности! Для предотвращения потери данных предварительно расшифруйте все зашифрованные таблицы!

Удаление объектов "Крипто БД 2.0" с сервера проводится штатным ПО конфигурации (мастер конфигурации). Для того, чтобы удалить объекты "Крипто БД 2.0" с сервера, выполните следующее:

* На АРМ администратора безопасности нажмите **Пуск** > (**Все**) **программы** > **Aladdin** > **CryptoDB** > **Конфигурирование КриптоБД** (рис. 8).
* В открывшемся окне диалога (рис. 9) нажмите **Далее**.
* В открывшемся окне (рис. 10) задайте имя строку связи с целевой БД, имя системной учетной записи БД (администратора БД) и пароль для системной учётной записи целевой базы данных.
* Для продолжения удаления нажмите **Далее**.

Примечание

Описаниеформата строки связи для сервера БД приведено в документации по администрированию целевой СУБД и для соответствующей версии ПО.

* Если вы готовы продолжить удаление, в окне выбора режима конфигурации (рис. 17) выберите **Удалить объекты Крипто БД**. Но если вы хотите исправить данные, введённые в предыдущем окне, нажмите **Назад** и вернитесь к шагу 3.

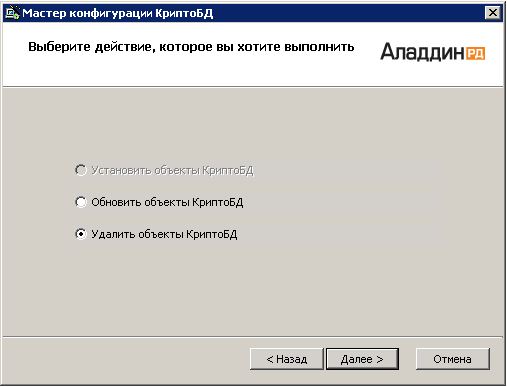


Рис. 17 — Удаление объектов "Крипто БД 2.0" с сервера. Выбор действия

* В окне готовности мастера нажмите **Удалить**.
* Удаление займёт некоторое время, по прошествии которого появится окно завершения процесса удаления (рис. 18). В этом окне нажмите **Готово**.

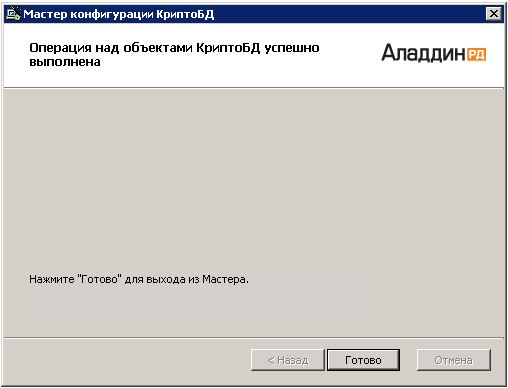


Рис. 18 — Удаление объектов "Крипто БД 2.0" с сервера. Завершение работы мастера

## Удаление ПО СКЗИ "Крипто БД 2.0" с АРМ администратора безопасности

Удаление ПО СКЗИ "Крипто БД 2.0" с АРМ администратора безопасности проводится штатной программой установки. Для того чтобы удалить ПО СКЗИ "Крипто БД 2.0" с АРМ администратора безопасности, выполните следующее:

1. С компакт-диска "Крипто БД 2.0" или с жёсткого диска АРМ администратора безопасности запустите С компакт-диска "Крипто БД 2.0" запустите файл:

* Aladdin.CryptoDB.Oracle.GOST.msi - для Oracle;
* Aladdin.CryptoDB.MSSQL.GOST.msi - для Microsoft SQL Server;
* Aladdin.CryptoDB.Tibero.GOST.msi - для Tibero.

Данный файл расположен в папках Win32 или x64 для версий OC Windows 32 или 64 bit соответственно.

Примечание

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

1. В открывшемся окне программы установки (рис. 19) нажмите **Далее**.

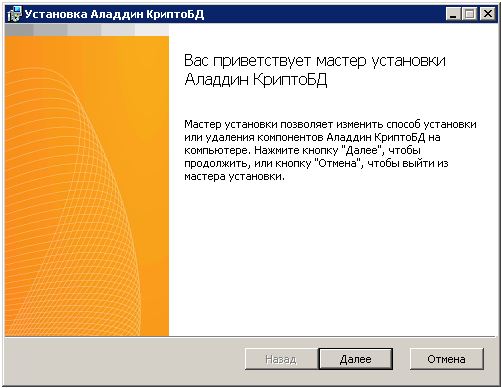


Рис. 19 — Удаление ПО "Крипто БД 2.0" с АРМ администратора безопасности. Начало удаления

1. В окне выбора режима работы программы установки (рис. 20) нажмите **Удалить.**

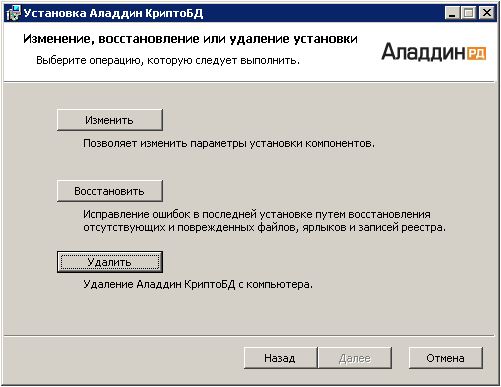


Рис. 20 — Удаление ПО СКЗИ "Крипто БД 2.0" с АРМ администратора безопасности. Выбор операции

1. В открывшемся окне (рис. 21) нажмите **Удалить.**

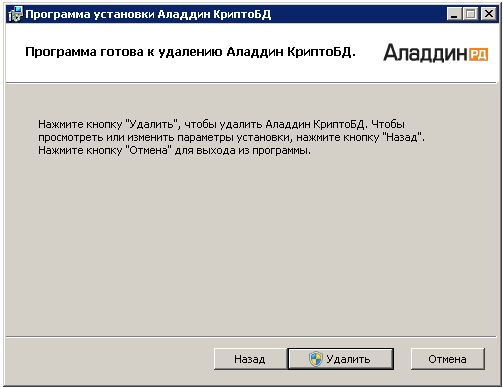


Рис. 21 — Удаление ПО СКЗИ "Крипто БД 2.0" с АРМ администратора безопасности. Подтверждение удаления

1. В окне завершения удаления (рис. 22) нажмите **Готово**.

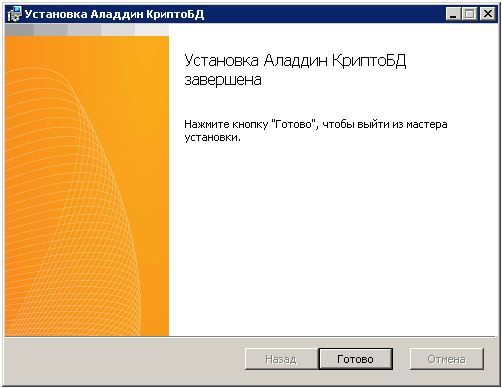


Рис. 22 — Удаление ПО СКЗИ "Крипто БД 2.0" с АРМ администратора безопасности. Завершение удаления

## Удаление ПО СКЗИ "Крипто БД 2.0" с АРМ пользователей

1. Удаление ПО СКЗИ "Крипто БД 2.0" с АРМ пользователей проводится штатными средствами. Для того чтобы ими воспользоваться, выполните следующее: С компакт-диска "Крипто БД 2.0" запустите файл (SLOra.msi - для Oracle, SLSql.msi - для MSSQL, SLTib.msi - для Tibero). Данный файл расположен в папках Win32 или x64 для версий OC Windows 32 или 64 bit соответственно.

Примечание

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

* В открывшемся окне мастера установки нажмите Далее.
* В окне выбора режима установки нажмите Удалить для удаления ПО СКЗИ "Крипто БД 2.0", Назад для возврата к предыдущему шагу (рис. 23).

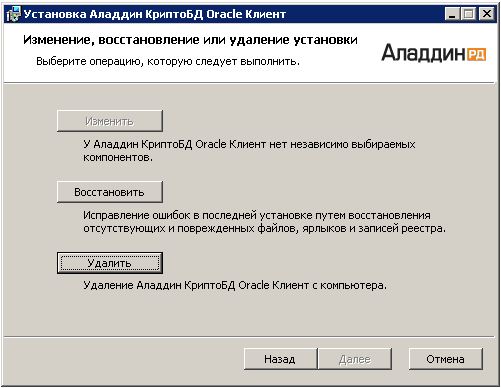


Рис. 23 — Удаление ПО СКЗИ "Крипто БД 2.0" с АРМ пользователя

* В окне подтверждения (рис. 24) нажмите Удалить. Нажмите Назад для возврата к предыдущему шагу.

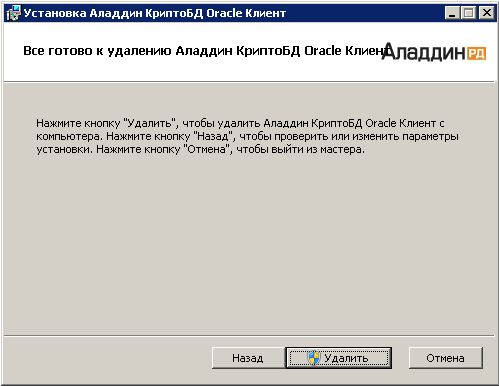


Рис. 24 — Удаление ПО СКЗИ "Крипто БД 2.0" с АРМ пользователя. Подтверждение удаления

* В окне завершения (рис. 25) нажмите Готово для завершения работы мастера установки.

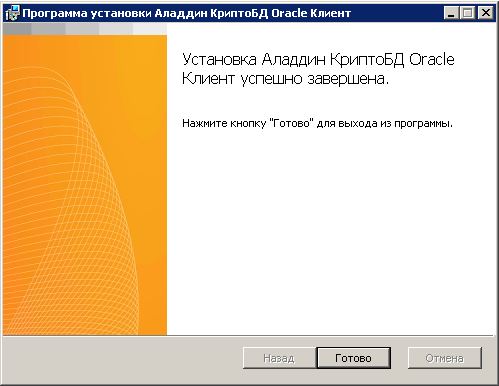


Рис. 25 — Удаление ПО СКЗИ "Крипто БД 2.0" с АРМ пользователя. Завершение удаления

### Удалённые процедуры установки

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

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

* файл **SL<DB>.msi** (**SLOra.msi** - для Oracle, **SLSql.msi** - для MSSQL, **SLTib.msi** - для Tibero);
* утилита **psexec.exe**, входящий в пакет **PsTools**.

Для того чтобы удалить ПО "Клиент Крипто БД" на удалённом компьютере, выполните следующие шаги:

* 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 /x <SL<DB>.msi>**

где:

* **<psexec>** — путь к утилите **psexec.exe**;
* **<computer>** — имя удалённого компьютера;
* **<SL<DB>.msi>** — сетевой путь к файлу установки для соответствующей платформы БД 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.

### Централизованные процедуры удаления

В домене Windows ПО "Клиент Крипто БД" можно удалять с помощью групповой политики. Например, при использовании Microsoft Windows Server 2003 или 2008 руководствуйтесь статьями базы знаний Microsoft [33] или [34] соответственно.

# Использование консоли администратора безопасности

## Назначение консоли

Консоль администратора безопасности — приложение для интерактивного выполнения следующих функций по обеспечению конфиденциальности информации, хранящейся в таблицах целевой базы данных:

* создание и смена ключей сервера базы данных;
* генерация, смена и удаление ключей шифрования;
* зашифрование и расшифрование информации в таблицах БД;
* управление ключами шифрования пользователей базы данных (приложений базы данных);
* резервное копирование и восстановление ключей шифрования;
* контроль целостности и восстановление объектов "Крипто БД 2.0";
* контроль целостности объектов пользователей БД;
* управление аудитом.

## Условия использования консоли

Приложение выполнено по технологии консоли управления Windows (рис. 28) и должно устанавливаться только на АРМ администратора безопасности. Администратор безопасности должен иметь заранее подготовленный USB-ключ или смарт-карту с установленными электронной лицензией Крипто БД, закрытым ключом и сертификатом (см. подраздел 7.2). Ключевая пара, соответствующая сертификату администратора безопасности, в дальнейшем будет использована для защиты ключей шифрования и ключей сервера БД.

## Соединение с целевой базой данных

Консоль администратора безопасности при каждом конкретном запуске может работать только с одним экземпляром целевой базы данных, где предполагается шифрование таблиц. Таких БД может быть несколько, их выбор происходит в процессе соединения с базой данных по уникальному имени — строке соединения, которые определены в настройках клиентского ПО целевой БД.

Для того чтобы установить соединение с целевой БД, выполните следующее:

* На АРМ администратора безопасности нажмите Пуск > (Все) Программы > Aladdin > CryptoDB > (целевая БД) > Консоль администрирования.
* В окне диалога подключения к целевой базе данных введите строку соединения (Имя службы), имя пользователя - администратора безопасности, его пароль и нажмите Войти (рис. 26).

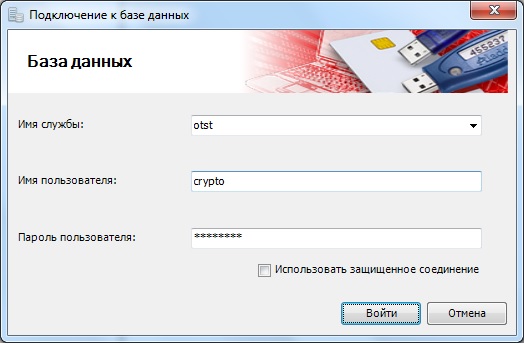


Рис. 26 — Консоль администратора безопасности. Ввод параметров соединения с целевой БД

Если подключение к целевой БД произошло успешно, откроется окно выбора сертификата администратора безопасности.

* В списке сертификатов выберите сертификат, который будет использоваться в данном сеансе соединения с базой данных, и нажмите **ОK** (рис. 27).
* При необходимости в открывшемся окне (рис. 45) введите PIN-код смарт-карты или USB-токена администратора безопасности и нажмите **ОК**.

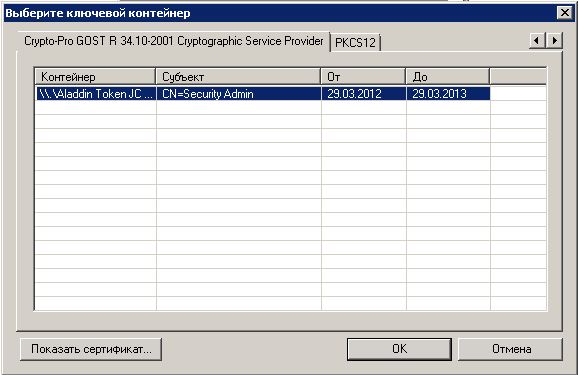


Рис. 27 — Консоль администратора безопасности. Выбор сертификата администратора безопасности

Примечания

* В случае если соединение с базой данных производится по защищённому протоколу, поддерживаемому целевой СУБД (SSL, Kerberos), отметьте флажок **Использовать защищённое соединение**. В этом случае ввод имени пользователя и пароля не требуется.
* В приведенном примере используется сертификат, созданный с помощью поставщика криптографии Крипто Про CSP (Crypto-Pro GOST 34.10-2001 Cryptographic Service Provider).
* Запрос PIN-кода происходит при расшифровании ключей сервера БД (если таковые были созданы) с помощью закрытого ключа администратора безопасности.

Общий вид главного окна приложения показан на рис. 28.

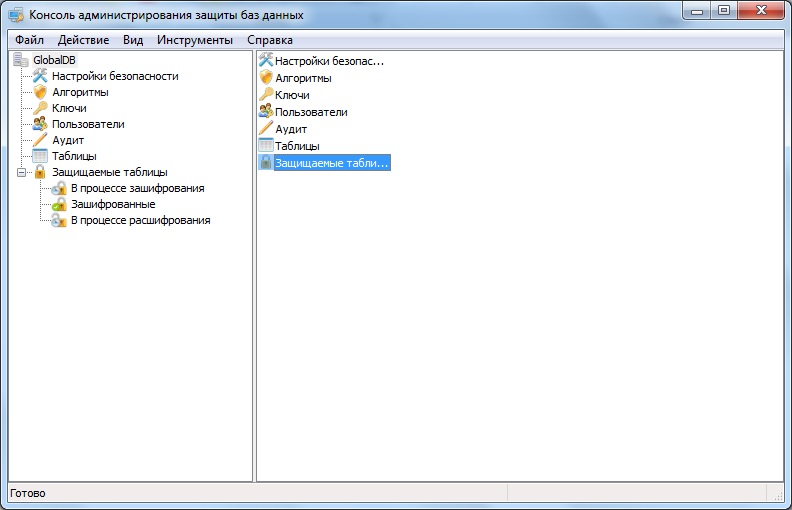


Рис. 28 — Консоль администратора безопасности. Главное окно приложения

## Управление ключами сервера БД

### Создание ключей сервера БД

Для безопасной передачи ключей шифрования с АРМ клиента на сервер БД их значения защищаются с использованием открытого ключа сервера базы данных. Входящий в библиотеку работы с ключами шифрования процесс — сервер ключей — на сервере базы данных расшифровывает полученный ключ шифрования своим закрытым ключом и передаёт полученное значение в сеанс пользователя. Ключевая пара сервера базы данных должна быть создана до процедуры генерации ключей шифрования. Каждому экземпляру базы данных должна соответствовать уникальная пара ключей, идентифицируемая именами хоста и экземпляра базы данных. Ключевые пары экземпляров, зашифрованные с использованием открытого ключа администратора безопасности, сохраняются на АРМ администратора безопасности в реестре Windows (в разделе **HKEY\_CURRENT\_USER\SOFTWARE\Aladdin\CryptoDB\<Целевая СУБД>\<host>\ <ID БД>\Server\Keys**).

Для генерации ключевой пары для сервера базы данных выполните следующее:

* В дереве консоли выберите корневой элемент **Настройки безопасности.** В правой панели выберите **Сервер ключей**, далееиз контекстного меню (щёлчок правой кнопки мыши) или из меню **Действие** выберите пункт **Свойства** (рис. 29).

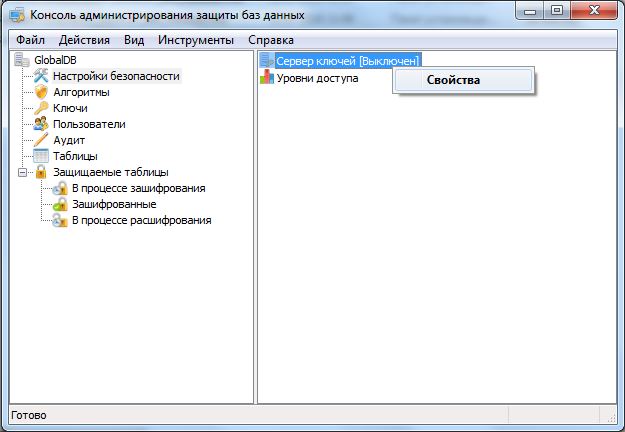


Рис. 29 — Консоль администратора безопасности. Обращение к интерфейсу настроек сервера

* В открывшемся окне настроек сервера (рис. 31) нажмите **Сгенерировать**.
* При необходимости следуйте инструкциям ДСЧ (рис. 30).

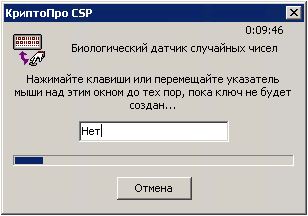


Рис. 30 — Окно биологического ДСЧ КриптоПро CSP

* В окне **Введите пароль** выберите алгоритм генерации открытого ключа (**OID открытого ключа**) задайте пароль для защиты закрытого ключа сервера БД, введя его в поле **Введите пароль** и в поле **Подтвердите пароль** (рис. 31).

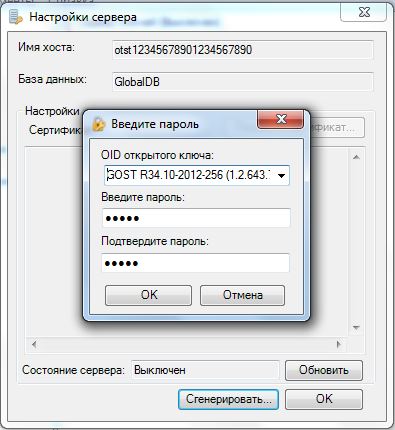


Рис. 31 — Регистрация пароля для защиты закрытого ключа сервера БД

* Нажмите **OK**.
* В окне **Параметры ключа** укажите параметры алгоритма генерации (рис. 32). Нажмите **Выбрать**.

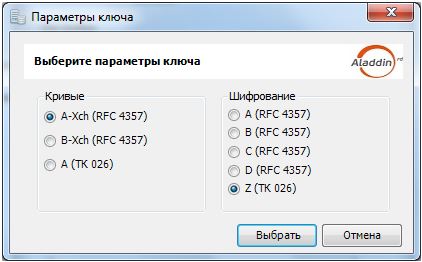


Рис. 32 — Консоль администратора безопасности. Параметры генерации ключей сервера

* В окне **Параметры контейнера** перейдите на вкладку **ГОСТ** и выберите параметры ключевого контейнера сервера ключей. Поля **Число итераций** установите в **1** (рис. 33). Нажмите **Выбрать**.

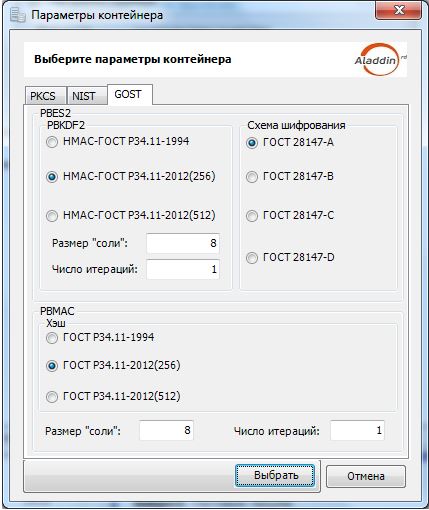


Рис. 33 — Консоль администратора безопасности. Параметры ключевого контейнера

* При необходимости введите PIN-код ключевого контейнера администратора безопасности (рис. 45).

Примечания

1. Перед выполнением операции генерации ключей сервера БД производится проверка целостности модулей серверной части Крипто БД. Это может занять некоторое время.
2. В целях обеспечения сохранности закрытого ключа сервера рекомендуется задавать пароль, соответствующий критериям, приведённым в разделе 17 настоящего руководства.
3. Наборы параметров алгоритмов генерации ключей изложены в [24],[29].
4. Наборы параметров ключевого контейнера приведены в [31],[32].

* В окне **Настройки сервера** в поле **Сертификат** отобразится значение сертификата сервера БД (рис. 34).

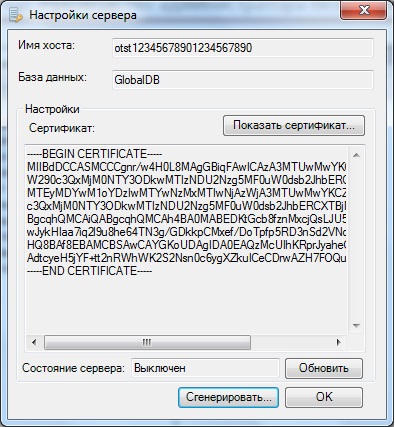


Рис. 34 — Консоль администратора безопасности. Генерация ключей сервера

* Для просмотра свойств сертификата нажмите **Показать сертификат...**.
* Для сохранения сгенерированной ключевой пары нажмите **ОК**.

Примечание

Рекомендуется сохранить резервные копии ключей сервера согласно инструкции, приведённой в документе RU.46538383.50 1430 005-01 92 01-2 "Крипто БД. Руководство администратора безопасности. Часть II".

### Смена ключей сервера БД

Смена ключей сервера производится администратором безопасности по истечении срока действия этих ключей либо в случае их компрометации. Для смены ключей сервера выполните следующую последовательность действий:

* С помощью консоли администратора безопасности остановите работу сервера ключей (см. п. 14.10.3).
* Выполните действия, перечисленные в п. 14.4.1. Все необходимые изменения в базе данных будут сделаны автоматически.
* Запустите сервер ключей (см. п. 14.10.2).

## Управление метками безопасности

Для того чтобы иметь возможность назначать метки конфиденциальности для зашифровываемых данных и метки безопасности для копий ключей пользователя, выполните предварительную настройку справочника меток. Для настройки справочника меток выполните следующее:

* В дереве консоли выберите корневой элемент **Настройки безопасности.** В правой панели выберите **Уровни доступа**, далееиз контекстного меню (щёлкнув правой кнопки мыши) или из меню **Действие** выберите пункт **Свойства**.
* В окне справочника меток отметьте метки, которые будут использоваться для управления доступом. При необходимости отредактируйте названия меток (Рис. 35).
* Нажмите **ОК** для сохранения изменений и закрытия окна, **Отмена** - для выхода без сохранения.

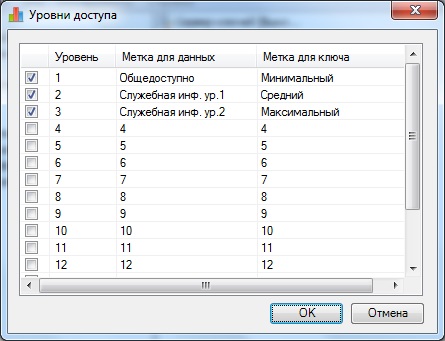


Рис. 35 — Консоль администратора безопасности. Справочник меток

Примечание

Количество меток фиксировано. Для "Крипто БД 2.0" текущей версии оно равно 16.

## Управление ключами шифрования

### Генерация ключей шифрования

Ключи шифрования могут быть созданы в произвольном количестве для последующего использования при шифровании колонок таблиц БД. Для создания ключа шифрования выполните следующее:

* В консоли администратора безопасности (рис. 28) выберите **Ключи**.
* Из контекстного меню (нажмите правую кнопку мыши), или из меню **Действие** выберите **Создать новый ключ...** (рис. 36).

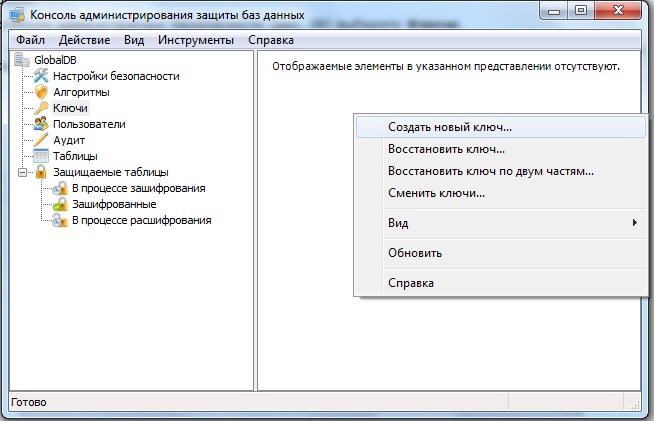


Рис. 36 — Консоль администратора безопасности. Генерация ключей шифрования

* В открывшемся окне (рис. 37) в поле **Имя ключа** введите имя ключа и из выпадающего списка выберите алгоритм шифрования, который будет использоваться с данным ключом.

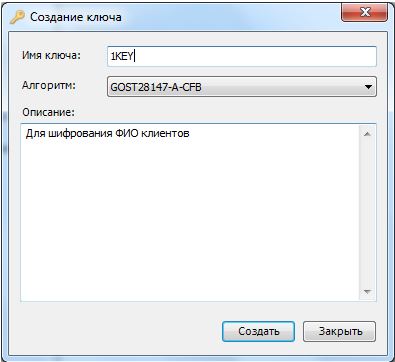


Рис. 37 — Консоль администратора безопасности. Создание ключа шифрования

* При необходимости в поле **Описание** введите описание создаваемого ключа.
* Для создания ключа с указанными свойствами нажмите **Создать**.
* При необходимости следуйте инструкциям ДСЧ (рис. 30).

Созданные ключи шифрования отобразятся в правой панели (рис. 38).

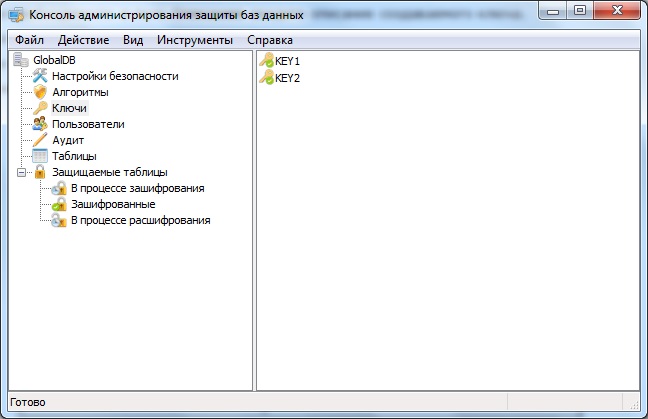


Рис. 38 — Консоль администратора безопасности. Созданные ключи шифрования

### Смена ключей шифрования

Смена ключей шифрования производится по истечении сроков их использования либо в случае их компрометации. Для смены ключей шифрования выполните следующую последовательность действий:

* Остановите работу сервера ключей (см. п. 14.10.2).
* Обратитесь к администратору целевой БД для завершения всех сеансов пользователей и автоматических процессов, работающих с зашифрованными таблицами, и подождите, пока администратор целевой БД завершит все такие сеансы.
* В консоли администратора безопасности (рис. 28) выберите **Ключи**.
* Из контекстного меню (нажмите правой кнопки мыши), или из меню **Действие** выберите **Смена ключей шифрования** (рис. 39).

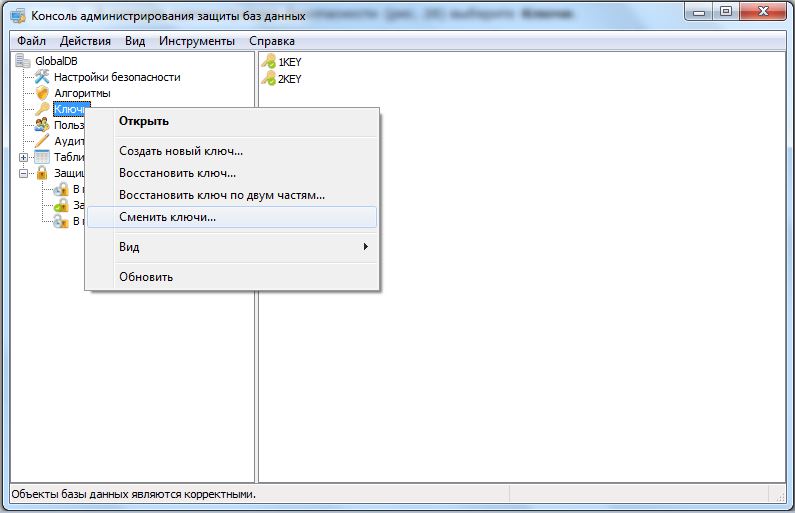


Рис. 39 — Консоль администратора безопасности. Смена ключей шифрования

* В открывшемся окне **Смена ключей** будет отображён список ключей шифрования (рис. 40). Если в этом списке есть ключи шифрования, которые подлежат смене, отметьте их и нажмите **Сменить**. В противном случае нажмите **Отмена**.

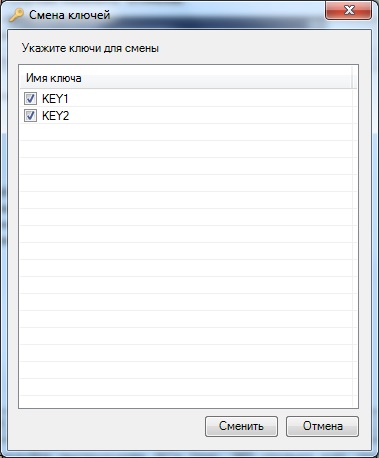


Рис. 40 — Консоль администратора безопасности. Выбор ключей шифрования для смены

* При необходимости следуйте инструкциям ДСЧ (рис. 30) столько раз, сколько ключей было выбрано для смены.
* По завершении процесса смены ключей шифрования появится окно с информацией о количестве сменённых ключей (рис. 41). В этом окне нажмите **ОК**.

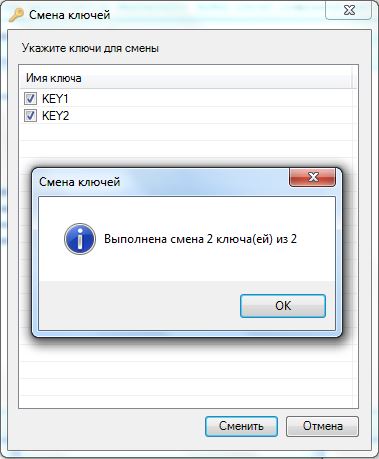


Рис. 41 — Консоль администратора безопасности. Завершение смены ключей шифрования

### Удаление ключа шифрования

Примечание

Ключ шифрования может быть удалён только в случае, когда нет ни одной колонки, зашифрованной с использованием данного ключа.

Для удаления из репозитория "Крипто БД 2.0" ключа шифрования и всех его пользовательских копий, выполните следующее:

* В консоли администратора безопасности (рис. 28) дважды щёлкните **Ключи**.
* Выберите ключ шифрования, который вы хотите удалить.
* Из контекстного меню (нажмите правой кнопкой мыши) или из меню **Действие** выберите **Удалить** (см. рис. 42).

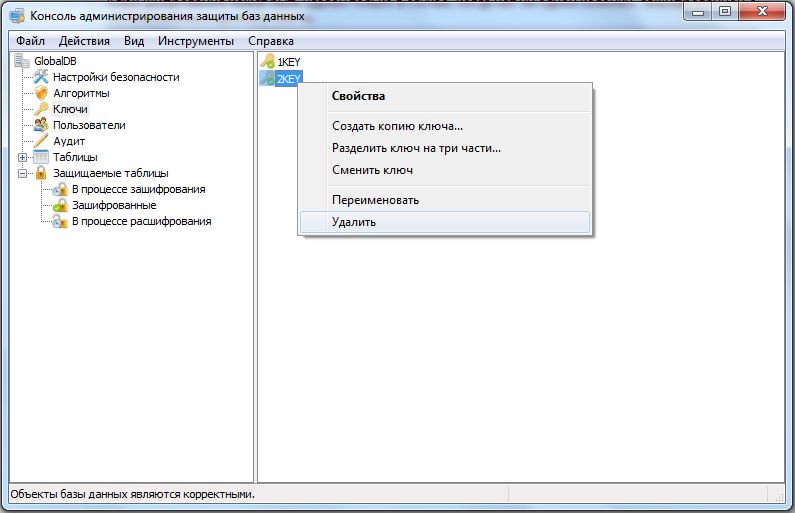


Рис. 42 — Консоль администратора безопасности. Удаление ключей шифрования

* В окне подтверждения убедитесь в том, что вы верно выбрали ключ для удаления. Если это не так, нажмите **Нет**. Если ключ для удаления выбран верно, нажмите **Да**.

## Шифрование данных

С целью минимизации времени простоя прикладных приложений, работающих с таблицами, колонки которых подлежат шифрованию (далее - **целевые таблицы**), процессы зашифрования, расшифрования или перешифрования (смена ключа шифрования) разделены на следующие этапы:

* подготовка к зашифрованию/расшифрованию/перешифрованию;
* зашифрование/расшифрование/перешифрование данных;
* завершение зашифрования/расшифрования/перешифрования.

На **этапе** 1 для целевой таблицы создаются дополнительные колонки, создаются или модифицируются промежуточные представления и триггеры. Дополнительные колонки создаются для каждой колонки целевой таблицы, подлежащей зашифрованию, расшифрованию или перешифрованию (далее - **целевые колонки**).

На **этапе 2** для администратором безопасности создаются задания для зашифрования, расшифрования или перешифрования данных. Эти задания могут быть выполнены как непосредственно после их создания, так и отложено, например, во время минимальной нагрузки на сервер базы данных. В рамках одного задания может быть также определено количество строк для обработки (все строки целевой таблицы, либо некоторая часть).

На **этапе 3** для целевой таблицы производятся некоторые завершающие действия, как правило автоматически. Так, например, завершение операции расшифрования предполагает удаление дополнительных колонок, представлений и триггеров.

### Условие выполнения операций шифрования данных

На время проведения операций шифрования (см. раздел 14.7) администратор целевой БД должен предоставить схеме пользователя – администратора безопасности дополнительные полномочия, список которых приведён в документах:

* RU.46538383.50 1430 005-01 92 02 "Крипто БД. Руководство администратора базы данных Oracle";
* RU.46538383.50 1430 005-01 92 03 "Крипто БД. Руководство администратора базы данных MSSQL";
* RU.46538383.50 1430 005-01 92 04 "Крипто БД. Руководство администратора базы данных Tibero".

### Подготовка таблицы к зашифрованию

После успешного завершения подготовки целевой таблицы к зашифрованию данные целевых колонок остаются незашифрованными. Операции над данными целевых колонок подчиняются следующим правилам:

* Выборка данных (select). При наличии у пользователя ключа шифрования для данной целевой колонки возвращаются либо расшифрованные данные из дополнительной колонки, либо ещё незашифрованные данные из целевой колонки. При отсутствии ключа шифрования всегда возвращается маскирующее значение (см. ниже);
* Вставка данных (insert). При наличии у пользователя ключа шифрования для данной целевой колонки данные, вставляемые в дополнительную колонку, будут зашифрованы соответствующим ключом. Целевая колонка заполняется маскирующим значением (см. ниже). При отсутствии ключа шифрования будет вызвано исключение, и операция завершится ошибкой;
* Обновление данных (update). При наличии у пользователя ключа шифрования для данной целевой колонки она заполняется маскирующим значением (см. ниже), а дополнительная колонка соответствующим зашифрованым значением. При отсутствии ключа шифрования будет вызвано исключение, и операция завершится ошибкой.

Для того, чтобы подготовить таблицу для зашифрования, выполните следующее:

* Порекомендуйте всем пользователя на время зашифрования прекратить работу с таблицей. Также рекомендуется завершить работу всех приложений, которые обращаются к целевой таблице.
* Сообщите администратору базы данных о необходимости резервного копирования таблицы и предоставления вам дополнительных полномочий, указанных в документах:
* RU.46538383.50 1430 005-01 92 02 "Крипто БД. Руководство администратора базы данных Oracle";
* RU.46538383.50 1430 005-01 92 03 "Крипто БД. Руководство администратора базы данных MSSQL";
* RU.46538383.50 1430 005-01 92 04 "Крипто БД. Руководство администратора базы данных Tibero".
* Дождитесь окончания резервного копирования и получения дополнительных полномочий.
* Убедитесь в том, что смарт-карта или USB-токен, содержащий закрытый ключ и сертификат администратора безопасности, подключён к АРМ. Если это не так, подключите его.
* В дереве консоли администратора безопасности (рис. 28) раскройте узел Таблицы.
* В открывшемся списке выберите схему.
* В отобразившемся в правой панели списке таблиц выбранной схемы выберите таблицу, которую следует подготовить к зашифрованию (рис. 43).

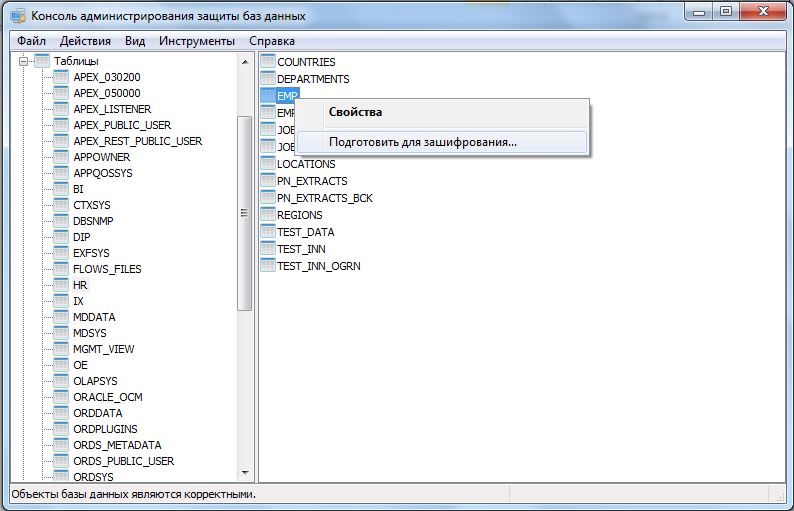


Рис. 43 — Консоль администратора безопасности. Выбор таблицы для подготовки

* Из контекстного меню (щёлкните правой кнопкой мыши) или меню **Действие** выберите **Подготовить для зашифрования**.
* В открывшемся окне со списком колонок таблицы для колонок, которые следует зашифровать, задайте пароль и подтверждение пароля (будет использоваться при создании заданий для зашифрования данных см. раздел 14.7.3), выберите ключи шифрования и метки безопасности шифруемых данных. При необходимости задайте в поле **Зашифрованное представление** согласно табл. 4 и табл. 5 шаблон маскирующего значения, определяющий формат подмены зашифрованных данных для пользователей и автоматических процессов, для которых не созданы ключи шифрования пользователей (рис. 44).

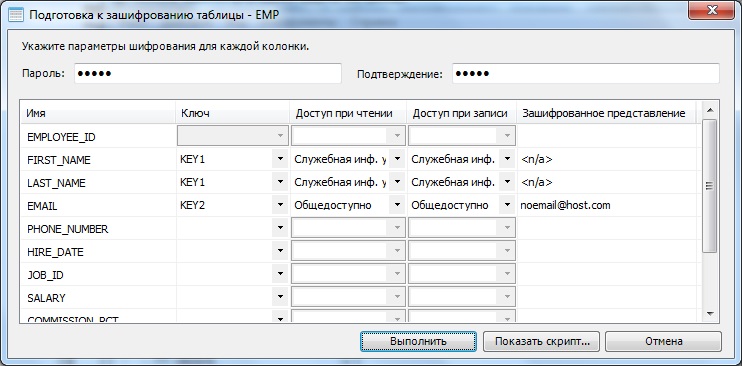


Рис. 44 — Консоль администратора безопасности. Выбор колонок для зашифрования

Табл. 4 — Шаблоны маскирующих значений (для целевых БД Oracle и Tibero)

| Тип зашифрованной колонки | Шаблон | Результат маскирования |
| --- | --- | --- |
| Текстовый/ бинарный | ‘строка’ | Указанная строка символов.  Может содержать произвольное количество макроподстановок вида:   * %D(N) — подставляется произвольное число, не превышающее N; * %S(N) — подставляется произвольная строка символов, длиной не более N;   Общая длина результирующего значения усекается до размера колонки. |
| NULL | NULL |
| Числовой | NULL | NULL |
| ‘константа’ | Значение указанной константы.  Точность усекается до значения шкалы колонки.  Неверное задание значения шаблона вызывает исключение -20011 (Invalid mask). |
| ‘X:Y’ | Случайное значение в интервале X…Y включительно.  X,Y – вещественные числа.  Точность усекается до значения шкалы колонки.  Неверное задание значения шаблона (X > Y, либо величины X или Y превышают разрядность колонки) вызывает исключение -20011 (Invalid mask). |
| Дата/время | NULL | NULL |
| ‘%SD’ | Значение системной даты (SYSDATE). |
| 'yyyymmddhh24miss-YYYYMMDDHH24MISS' | Случайное время в заданном интервале дат.  yyyy, YYYY — четыре цифры года  mm, MM — две цифры месяца (01..12)  dd, DD — две цифры дня (01..31)  hh24, HH24 — две цифры часов (00..23)  mi, MI — две цифры минут (00..59)  ss, SS — две цифры секунд (00..59).  Неверное задание значения шаблона вызывает исключение -20011 (Invalid mask). |
| Шаблон | Результат маскирования |
| ‘строка символов’ | Указанная строка символов.  Может содержать произвольное количество макроподстановок вида:   * %D(N) — подставляется произвольное число, не превышающее N; * %S(N) — подставляется произвольная строка символов, длиной не более N;   Общая длина результирующего значения усекается до размера колонки. |
| NULL | NULL |
| NULL | NULL |
| ‘константа’ | Значение указанной константы.  Точность усекается до значения шкалы колонки.  Неверное задание значения шаблона вызывает исключение -20011 (Invalid mask). |
| ‘X:Y’ | Случайное значение в интервале X…Y включительно.  X,Y – вещественные числа.  Точность усекается до значения шкалы колонки.  Неверное задание значения шаблона (X > Y, либо величины X или Y превышают разрядность колонки) вызывает исключение -20011 (Invalid mask). |
| NULL | NULL |
| ‘%SD’ | Значение системной даты (SYSDATE). |
| 'yyyymmddhh24miss-YYYYMMDDHH24MISS' | Случайное время в заданном интервале дат.  yyyy, YYYY — четыре цифры года  mm, MM — две цифры месяца (01..12)  dd, DD — две цифры дня (01..31)  hh24, HH24 — две цифры часов (00..23)  mi, MI — две цифры минут (00..59)  ss, SS — две цифры секунд (00..59).  Неверное задание значения шаблона вызывает исключение -20011 (Invalid mask). |

Табл. 5 — Шаблоны маскирующих значений (для целевой БД MS SQL)

| Тип зашифрованной колонки | Шаблон | Результат маскирования |
| --- | --- | --- |
| Текстовый | ‘строка’ | Указанная строка символов.  Может содержать произвольное количество макроподстановок вида:   * %D(N) — подставляется произвольное число, не превышающее N; * %S(N) — подставляется произвольная строка символов в верхнем регистре, длиной не более N; * превышающее N; * %s(N) — подставляется произвольная строка символов в нижнем регистре, длиной не более N; * %% - символ процента   Общая длина результирующего значения усекается до размера колонки. |
| NULL | NULL |
| Бинарный | Литерал,  %S(N), (%s(N)) | Литерал из шестнадцатеричных цифр;  Случайная строка символов, длиной не более N. |
| NULL | NULL |
| Числовой | NULL | NULL |
| ‘константа’ | Значение указанной константы.  Точность усекается до значения шкалы колонки.  Неверное задание значения шаблона вызывает исключение -20011 (Invalid mask). |
| ‘X:Y’, %D(N) | Случайное значение в интервале X…Y включительно.  X,Y – целые или вещественные числа, в зависимости от типа колонки.  Точность усекается до значения шкалы колонки.  Неверное задание значения шаблона (X > Y, либо величины X или Y превышают разрядность колонки) вызывает исключение -20011 (Invalid mask).  %D(N) - произвольное число, не превышающее N. Целое или вещественное, в зависимости от типа колонки. |
| Дата/время | NULL | NULL |
| ‘%SD’ | Значение системной даты (SYSDATE). Формат зависит от настроек ОС Windows. |
| Идентификатор (UID) | ‘%SD’ | %SD - уникальное случайное значение.  например, '6F9619FF-8B86-D011-B42D-00C04FC964FF' |

Важно

Задание непустого маскирующего значения обязательно для колонок, имеющих ограничение **NOT NULL**.

Примечания

1. Колонки, которые не могут быть зашифрованы, не отображаются в списке.
2. Колонки, которые могут быть зашифрованы, но содержат ограничения целостности, запрещены для выбора.
3. Полный список ограничений для шифрования приведен в документах:

* RU.46538383.50 1430 005-01 92 02 "Крипто БД. Руководство администратора базы данных Oracle";
* RU.46538383.50 1430 005-01 92 03 "Крипто БД. Руководство администратора базы данных MSSQL";
* RU.46538383.50 1430 005-01 92 04 "Крипто БД. Руководство администратора базы данных Tibero".

1. Маскирующие значения используются для обеспечения корректной работы приложений при обращении к зашифрованным данным без ключа шифрования, а также для сокрытия того факта, что данные являются зашифрованными.

* Если вы хотите просмотреть сценарий подготовки к зашифрованию, нажмите **Показать скрипт...**.
* Для того чтобы подготовить таблицу к зашифрованию выбранных колонок с использованием соответствующих им ключей, нажмите **Выполнить**.
* При необходимости в открывшемся окне (рис. 45) введите PIN-код смарт-карты или USB-токена администратора безопасности и нажмите **ОК**.

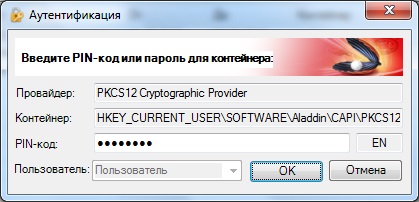


Рис. 45 — Ввод PIN –кода смарт-карты или USB-токена

Примечание

Запрос PIN-кода происходит во время получения ключей шифрования, которые защищены с использованием закрытого ключа администратора безопасности, содержащегося в ключевом контейнере, смарт-карте или USB-токене.

* В окне сообщения об окончании процесса подготовки к зашифрованию нажмите **ОК**.
* Подготовленная таблица отобразится в списке узла **Защищаемые таблицы/В процессе зашифрования** в формате <схема>.<таблица>(рис. 46).

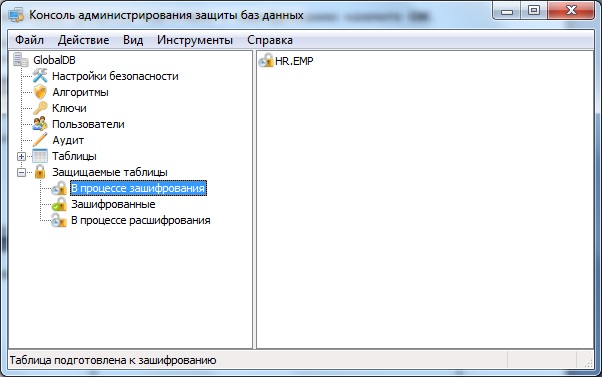


Рис. 46 — Консоль администратора безопасности. Завершение подготовки таблицы

* Сообщите пользователям о завершении подготовки к зашифрованию таблицы и о необходимости обращаться к ней посредством ПО СКЗИ "Крипто БД 2.0", установленного на их АРМ.

### Зашифрование данных в таблице

Данный этап может выполняться в несколько приёмов, в зависимости от объёма целевой таблицы и планирования зашифрования. После успешного завершения зашифрования (выполнения всех сформированных заданий) данные целевых колонок будут заполнены маскирующим значением, которое было задано на этапе подготовки к зашифрованию (см. раздел 14.7.2). Дополнительные колонки будут содержать соответствующие зашифрованные значения. Операции над данными целевых колонок подчиняются следующим правилам:

* Выборка данных (select). При наличии у пользователя ключа шифрования для данной целевой колонки возвращаются расшифрованные данные из дополнительной колонки. При отсутствии ключа шифрования возвращается маскирующее значение;
* Вставка данных (insert). При наличии у пользователя ключа шифрования для данной целевой колонки данные, вставляемые в дополнительную колонку, будут зашифрованы соответствующим ключом. Целевая колонка заполняется маскирующим значением. При отсутствии ключа шифрования будет вызвано исключение, и операция завершится ошибкой;
* Обновление данных (update). При наличии у пользователя ключа шифрования дополнительная колонка заполняется соответствующим зашифрованым значением. При отсутствии ключа шифрования будет вызвано исключение, и операция завершится ошибкой.

Для того, чтобы подготовить и выполнить задания для зашифрования целевых колонок, выполните следующее:

* Убедитесь в том, что смарт-карта или USB-токен, содержащий закрытый ключ и сертификат администратора безопасности, подключён к АРМ. Если это не так, подключите его.
* В дереве консоли администратора безопасности (рис. 28) раскройте узел **Защищаемые таблицы/В процессе зашифрования**.
* В отобразившемся в правой панели списке подготовленных таблиц выберите таблицу, колонки которой следует зашифровать (рис. 47).

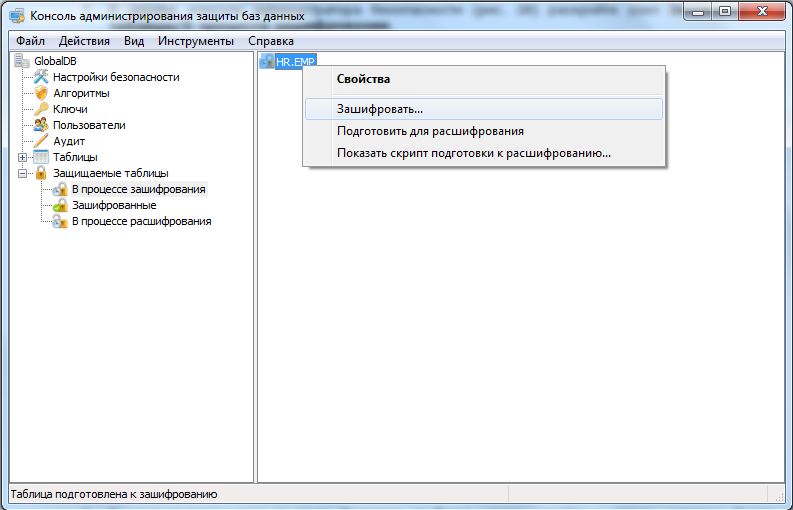


Рис. 47 — Консоль администратора безопасности. Выбор таблицы для зашифрования данных

* Из контекстного меню (щёлкните правой кнопкой мыши) или меню **Действие** выберите **Зашифровать...**.
* В открывшемся окне в поле **Условие выбора строк** задайте условие, которое будет использоваться для выбора части строк целевой таблицы, предназначенные для зашифрования в рамках создаваемого задания. В поле **Размер блока выборки** укажите количество строк, после которого будет производится фиксация изменений в БД (commit). Если возможно зашифрование всех строк таблицы, то отметьте пункт выбора **Все строки таблицы** (рис. 48).
* Для просмотра сценария задания на зашифрование нажмите кнопку **Показать скрипт...**, для выполнения задания - кнопку **Выполнить** (рис. 48).

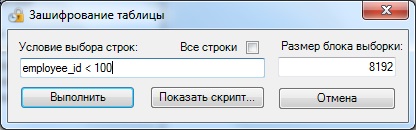


Рис. 48 — Консоль администратора безопасности. Выбор условия для задания на зашифрование

* Для просмотра сценария задания на зашифрование нажмите кнопку **Показать скрипт...**, для выполнения задания - кнопку **Выполнить** (рис. 48).
* Обработка задания займёт некоторое время, в зависимости от результирующего количества строк, определённого условием выбора. В окне сообщения об окончании обработки задания нажмите **ОК**.
* Для просмотра результата работы задания в дереве консоли администратора безопасности (рис. 28) раскройте узел **Таблицы**. В открывшемся списке выберите схему. В отобразившемся в правой панели списке таблиц выбранной схемы выберите таблицу. Из контекстного меню (щёлкните правой кнопкой мыши) или меню **Действие** выберите **Свойства...**. В открывшемся окне свойств таблицы перейдите на вкладку **Зашифрованные колонки**. В списке отобразится следующая информация (рис. 49):
* наименование колонки;
* наименование ключа шифрования, с помощью которого колонка зашифрована;
* метки доступа на чтение и запись;
* процент зашифрованных строк по отношению к общему количеству строк таблицы. Общее количество строк можно посмотреть на вкладке **Общие** (рис. 49);
* маскирующее значение для колонки (Представление).

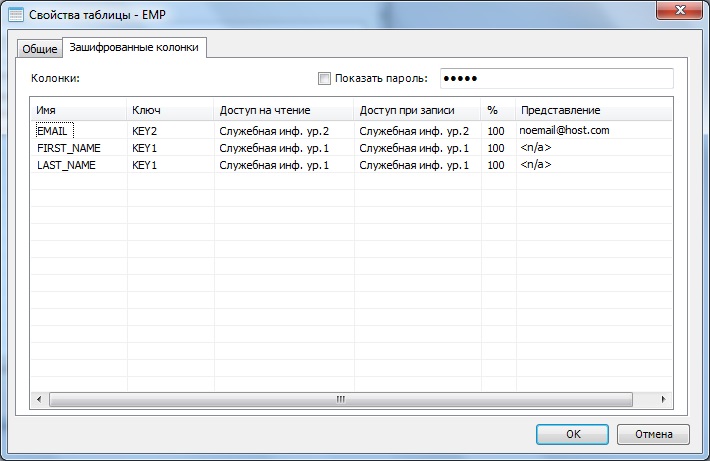


Рис. 49 — Консоль администратора безопасности. Просмотр свойств таблицы

* Для закрытия окна нажмите **ОК** или **Отмена**.
* Для последовательного формирования заданий на зашифрование выполняйте п.п. 1..8 до полного зашифрования строк целевой таблицы.
* После зашифрования всех строк и колонок целевой таблицы, она отобразится в списке узла **Защищаемые таблицы/Зашифрованные** (рис. 50). Сообщите администратору базы данных о необходимости изъятия дополнительных полномочий, назначенных ранее (см. раздел 14.7.2).

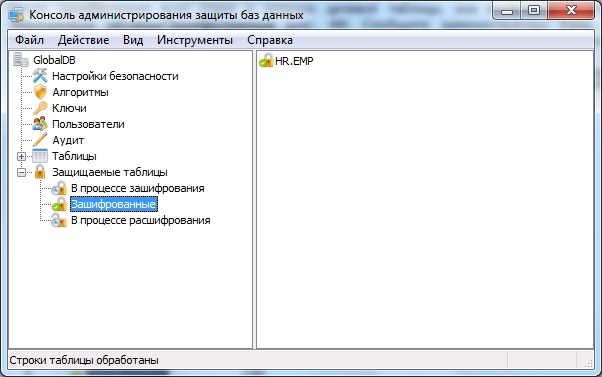


Рис. 50 — Консоль администратора безопасности. Окончание зашифрования данных

### Подготовка таблицы к расшифрованию

После успешного завершения подготовки целевой таблицы к расшифрованию целевые колонки содержат маскирующие значения. Операции над данными целевых колонок подчиняются следующим правилам:

* Выборка данных (select). При наличии у пользователя ключа шифрования для данной целевой колонки возвращаются либо расшифрованные данные из дополнительной колонки, либо уже расшифрованные данные из целевой колонки. При отсутствии ключа шифрования всегда возвращается маскирующее значение (см. раздел 14.7.2);
* Вставка данных (insert). Данные в дополнительную колонку не вставляются, целевая колонка заполняется вставляемым значением;
* Обновление данных (update). При наличии у пользователя ключа шифрования для данной целевой колонки она заполняется вставляемым значением, дополнительная колонка не меняется. При отсутствии ключа шифрования и при условии, что данная строка ещё не расшифрована, будет вызвано исключение, и операция завершится ошибкой.

Для того, чтобы подготовить таблицу для расшифрования, выполните следующее:

* Порекомендуйте всем пользователя на время расшифрования прекратить работу с целевой таблицей. Также рекомендуется завершить работу всех приложений, которые обращаются к целевой таблице.
* Сообщите администратору базы данных о необходимости резервного копирования таблицы и предоставления вам дополнительных полномочий, указанных в документах:
* RU.46538383.50 1430 005-01 92 02 "Крипто БД. Руководство администратора базы данных Oracle";
* RU.46538383.50 1430 005-01 92 03 "Крипто БД. Руководство администратора базы данных MSSQL";
* RU.46538383.50 1430 005-01 92 04 "Крипто БД. Руководство администратора базы данных Tibero".
* Дождитесь окончания резервного копирования и получения дополнительных полномочий.
* Убедитесь в том, что смарт-карта или USB-токен, содержащие закрытый ключ и сертификат администратора безопасности, подключён к АРМ. Если это не так, подключите его.
* В дереве консоли администратора безопасности (рис. 28) выберите папку **Защищаемые таблицы/Зашифрованные**.
* В отобразившемся в правой панели списке выберите зашифрованную таблицу, которую следует подготовить к расшифрованию. Из контекстного меню (щёлкните правой кнопкой мыши) или меню **Действие** выберите **Подготовить для расшифрования**. (рис. 51).

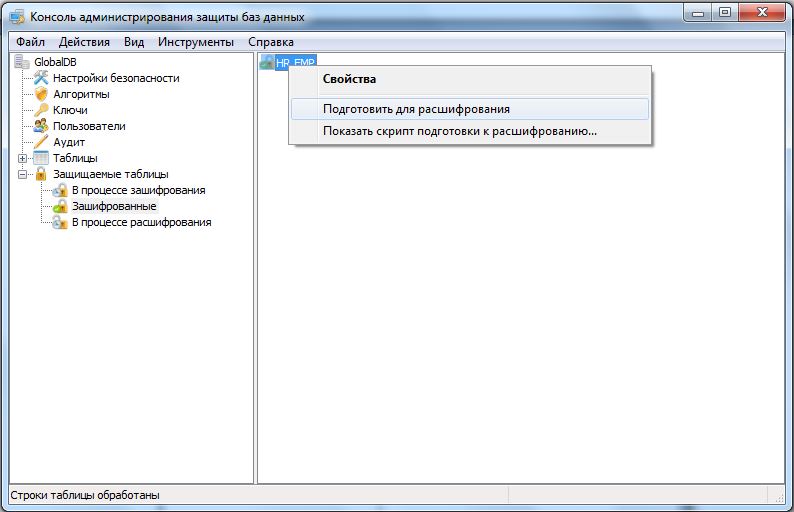


Рис. 51 — Консоль администратора безопасности. Подготовка таблицы к расшифрованию

* В окне подтверждения убедитесь в том, что вы верно выбрали целевую таблицу. Если это так, нажмите **Да**, чтобы начать подготовку таблицы. В противном случае нажмите **Нет**.
* При необходимости в открывшемся окне (рис. 45) введите PIN-код смарт-карты или USB-токена администратора безопасности и нажмите **ОК**.
* В окне сообщения о завершении процедуры подготовки к расшифрованию нажмите **ОК**.
* После завершения подготовки имя целевой таблицы отображаться в списке таблиц, находящихся в процессе расшифрования, в формате <схема>.<таблица> (рис. 52).

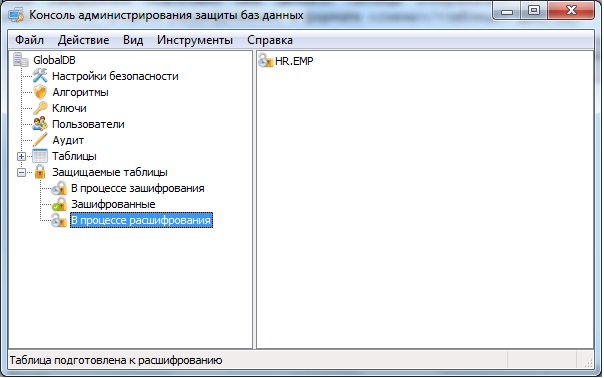


Рис. 52 — Консоль администратора безопасности. Завершение подготовки таблицы к расшифрованию

* Сообщите пользователям о завершении подготовки к расшифрованию таблицы.

### Расшифрование данных в таблице

Данный этап может выполняться в несколько приёмов, в зависимости от объёма целевой таблицы и планирования расшифрования. После успешного завершения расшифрования (выполнения всех сформированных заданий) данные целевых колонок будут заполнены расшифрованным значением. Дополнительные колонки будут помечены как неиспользуемые. Операции над данными целевых колонок подчиняются следующим правилам (при условии, что не все строки расшифрованы):

* Выборка данных (**select**). При наличии у пользователя ключа шифрования для данной целевой колонки возвращаются расшифрованные данные из дополнительной колонки, либо данные целевой колонки, если данныя строка расшифрована. При отсутствии ключа шифрования возвращается маскирующее значение;
* Вставка данных (**insert**).Целевая колонка заполняется соответствующим значением;
* Обновление данных (**update**). При наличии у пользователя ключа шифрования целевая колонка заполняется соответствующим значением. При отсутствии ключа шифрования и при условии, что данная строка не расшифрована, будет вызвано исключение, и операция завершится ошибкой.

Для того, чтобы подготовить и выполнить задания для расшифрования целевых колонок, выполните следующее:

* Убедитесь в том, что смарт-карта или USB-токен, содержащий закрытый ключ и сертификат администратора безопасности, подключён к АРМ. Если это не так, подключите его.
* В дереве консоли администратора безопасности (рис. 28) раскройте узел **Защищаемые таблицы/В процессе расшифрования**.
* В отобразившемся в правой панели списке подготовленных таблиц выберите таблицу, колонки которой следует расшифровать (рис. 53).

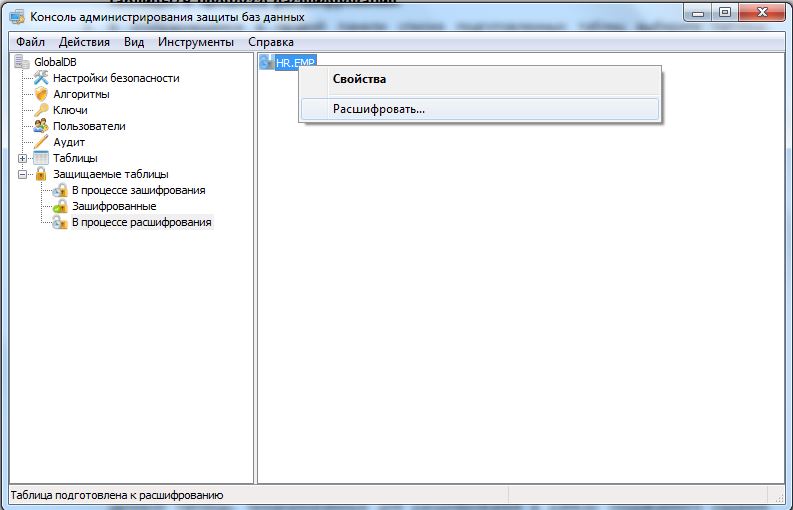


Рис. 53 — Консоль администратора безопасности. Выбор таблицы для расшифрования данных

* Из контекстного меню (щёлкните правой кнопкой мыши) или меню **Действие** выберите **Расшифровать...**.
* В открывшемся окне задайте условие, которое будет использоваться для выбора части строк целевой таблицы, предназначенные для расшифрования в рамках создаваемого задания. Если возможно расшифрование всех строк таблицы, то отметьте пункт выбора **Все строки таблицы** (рис. 54).
* Для просмотра сценария задания на расшифрование нажмите кнопку **Показать скрипт...**, для выполнения задания - кнопку **Выполнить** (рис. 54).

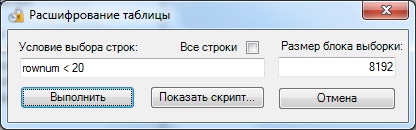


Рис. 54 — Консоль администратора безопасности. Выбор условия для задания количества строк на расшифрование

* Для просмотра сценария задания на зашифрование нажмите кнопку **Показать скрипт...**, для выполнения задания - кнопку **Выполнить** (рис. 54).
* Обработка задания займёт некоторое время, в зависимости от результирующего количества строк, определённого условием выбора. В окне сообщения об окончании обработки задания нажмите **ОК**.
* Для просмотра результата работы задания в дереве консоли администратора безопасности (рис. 28) раскройте узел **Таблицы**. В открывшемся списке выберите схему. В отобразившемся в правой панели списке таблиц выбранной схемы выберите таблицу. Из контекстного меню (щёлкните правой кнопкой мыши) или меню **Действие** выберите **Свойства...**. В открывшемся окне свойств таблицы перейдите на вкладку **Зашифрованные колонки**. В списке отобразится следующая информация (рис. 55):
* наименование колонки;
* пустое наименование ключа шифрования, так как таблица в процессе расшифрования;
* метки доступа на чтение и запись;
* процент зашифрованных строк по отношению к общему количеству строк таблицы. Общее количество строк можно посмотреть на вкладке **Общие** (рис. 55);
* маскирующее значение для колонки (Представление).

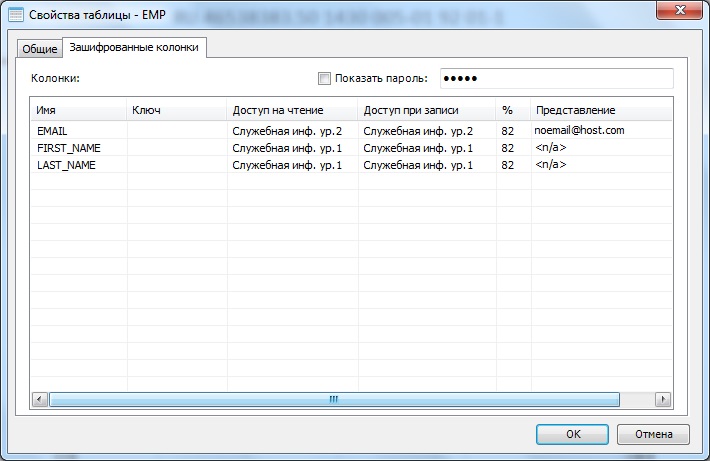


Рис. 55 — Консоль администратора безопасности. Просмотр свойств таблицы

* Для закрытия окна нажмите **ОК** или **Отмена**.
* Для последовательного формирования заданий на расшифрование выполняйте предыдущие п.п. до полного расшифрования строк целевой таблицы.
* После расшифрования всех строк и колонок целевой таблицы, она отобразится в списке узла **Таблицы/<**Схема**>** (рис. 43). Сообщите администратору базы данных о необходимости изъятия дополнительных полномочий, назначенных ранее (см. раздел 14.7.2).

## Управление пользователями Крипто БД

### Общие сведения о пользователях Крипто БД

Пользователем Крипто БД (далее по тексту - пользователь) считается любой субъект (человек, приложение), вне зависимости от наличия или отсутствия прав доступа к зашифрованным данным, предоставляемыми средствами ограничения доступа целевой БД. Пользователи Крипто БД, которым предоставлен доступ к зашифрованным данным (либо для которых планируется предоставление доступа), идентифицируются своими сертификатами открытого ключа. Все прочие пользователи идентифицируются именами или данными, допустимыми для аутентификации в целевой БД.

Сведения о ключевых контейнерах приложения приведены в документе RU.46538383.50 1430 005-01 92 01-2 "Крипто БД. Руководство администратора безопасности. Часть II".

Примечание

Пользователь может быть создан только после создания ключей сервера для целевой БД . См. раздел 14.4.1.

### Создание пользователя

Для того чтобы создать пользователя, выполните следующее:

* В консоли администратора безопасности (рис. 28) выберите **Пользователи**.
* В правой панели из контекстного меню (правая кнопка мыши) или меню **Действие** выберите **Создать пользователя...** (рис. 56).

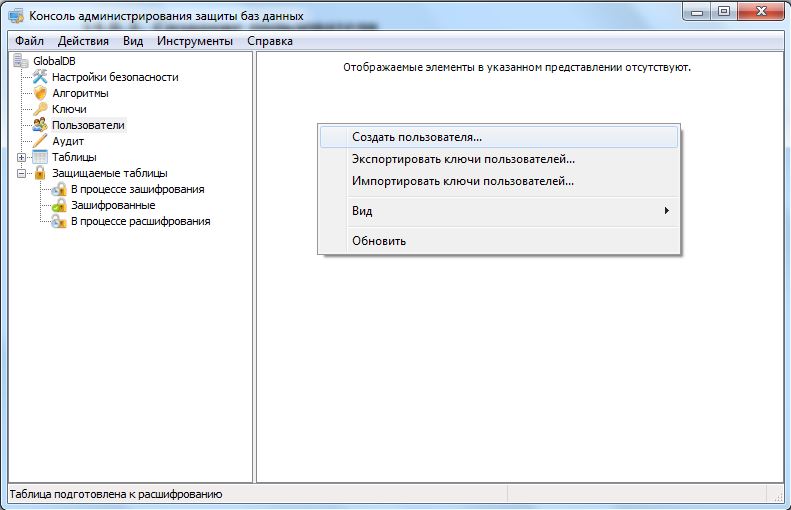


Рис. 56 — Консоль администратора безопасности. Создание пользователя

* В открывшемся окне **Создание пользователя** нажмите **Выбрать...** для выбора сертификата (ключевого контейнера) пользователя или ключевого контейнера приложения (рис. 57).

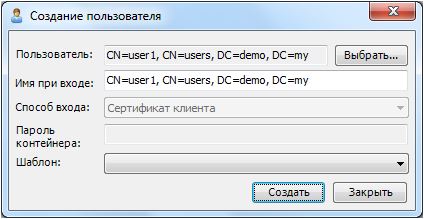


Рис. 57 — Консоль администратора безопасности. Диалог создания пользователя

* В стандартном окне диалога выбора файла выберите сертификат или ключевой контейнер и нажмите **Открыть**.
* Отличительное имя сертификата пользователя (выбранного как файл или извлечённого из контейнера) отобразится в поле **Пользователь** (рис. 57). Заполнение остальных полей формы зависит от выбора пользователя - сертификат или контейнер. Возможные варианты приведены в табл. 6.

Табл. 6 — Варианты создания пользователя

|  |  |  |
| --- | --- | --- |
| Поле формы | Выбранный тип файла | |
| Сертификат (\*.crt, \*.cer) | Контейнер (\*.p12, \*.pfx) |
| **Пользователь** | Отличительное имя в сертификате (поле Subject) | Отличительное имя в сертификате (поле Subject), извлечённом из контейнера |
| **Имя при входе** | Идентификатор пользователя в Крипто БД. По умолчанию равен отличительному имени в сертификате (поле Subject) | Идентификатор пользователя в Крипто БД. По умолчанию равен отличительному имени в сертификате (поле Subject) ), извлечённом из контейнера |
| **Способ входа** | **Сертификат клиента** (недоступно для изменения). Предполагается наличие у пользователя смарт-карты или USB-токена с личным ключом, соответствующим выбранному сертификату. Для получения доступа к ключам шифрования требуется ввод PIN-кода. | **Сертификат клиента**. Предполагается наличие у пользователя смарт-карты или USB-токена с ключевым контейнером, соответствующим выбранному. Для получения доступа к ключам шифрования требуется ввод PIN-кода.  **Контейнер на сервере**.  Предполагается хранение ключевого контейнера пользователя на сервере целевой БД. Для получения доступа к ключам шифрования требуется ввод PIN-кода контейнера.  **Контейнер на сервере с сохранением пароля**.  Предполагается хранение ключевого контейнера пользователя на сервере целевой БД. Для получения доступа к ключам шифрования ввод PIN-кода контейнера не требуется. Такой пользователь соответствует автоматизированным процессам, которые должны работать с зашифрованной информацией без участия человека. |
| **Пароль контейнера** | Не требуется | Требуется только для способа входа **Контейнер на сервере с сохранением пароля.** Должен совпадать с PIN-кодом выбранного ключевого контейнера. |

* Для создания пользователя, идентифицируемого данным сертификатом (ключевым контейнером) нажмите **Создать**, для отказа от создания - **Закрыть**. Отличительное имя созданного пользователя отобразится в правой панели консоли (папка **Пользователи**).

### Создание пользователя с заданием шаблона

Использование имеющегося пользователя в качестве шаблона позволяет создавать пользователя, идентифицируемого своим сертификатом и имеющего набор ключей шифрования (см. п. 14.9) как у шаблонного. Для того чтобы создать пользователя по шаблону, выполните следующее:

1. Выполните действия шагов 1-3 п. 14.8.2.
2. В списке выбора **Шаблон** выберите отличительное имя пользователя, используемого в качестве шаблона (рис. 57).
3. Для создания пользователя, идентифицируемого данным сертификатом (ключевым контейнером) нажмите **Создать**, для отказа от создания - **Закрыть**.

## Управление ключами шифрования пользователей

### Общие сведения о ключах пользователей

Для работы с зашифрованными данными каждому пользователю (приложению) необходимо предоставить доступ к ключам шифрования. Такой доступ предоставляется с помощью создания копий ключей шифрования для пользователей (далее — "ключ пользователя"). Создание ключа пользователя подразумевает зашифрование значения ключа шифрования с использованием открытого ключа, извлекаемого из сертификата пользователя или ключевого контейнера приложения. Сведения о ключевых контейнерах приложения приведены в документе RU.46538383.50 1430 005-01 92 01-2 "Крипто БД. Руководство администратора безопасности. Часть II".

### Создание ключей пользователя (первый способ)

Данный способ позволяет создать копии одного или нескольких ключей шифрования для выбранного пользователя. Такой способ может использоваться, например, в случае создания нового пользователя и необходимости создания для него некоторого набора копий имеющихся ключей шифрования. Для того чтобы создать ключи пользователя, выполните следующее:

1. В консоли администратора безопасности (рис. 28) раскройте папку **Пользователи**. В правой панели выберите пользователя, для которого создаются ключи, и откройте окно его свойств одним из следующих способов:

* дважды щёлкните; щёлкните правой кнопкой мыши и выберите **Свойства** (рис. 58);
* в меню **Действие** выберите **Свойства**.

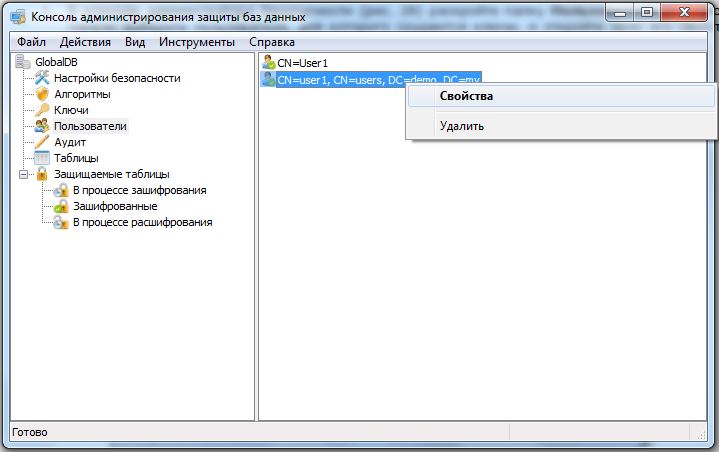


Рис. 58 — Консоль администратора безопасности. Свойства пользователя

1. В окне **Свойства пользователя** перейдите на вкладку **Ключи** и нажмите **Добавить...** (рис. 59).

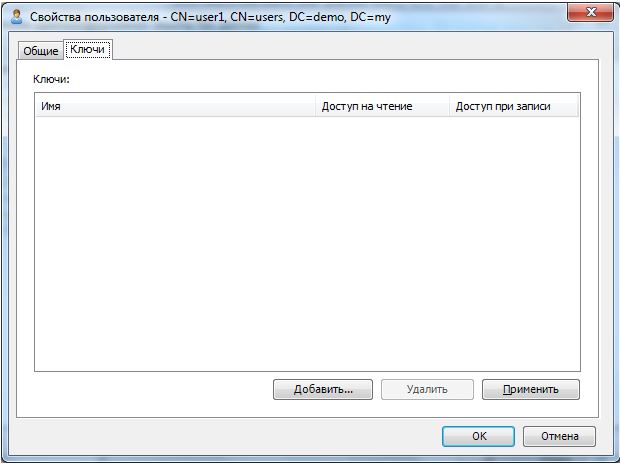


Рис. 59 — Консоль администратора безопасности. Ключи пользователя

1. В окне **Выбор ключей** отметьте те ключи шифрования, которые будут созданы для пользователя. Нажмите **ОК** для добавления выбранных ключей или **Отмена** для закрытия окна (рис. 60).

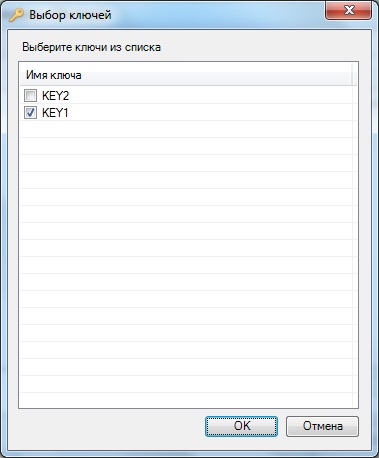


Рис. 60 — Консоль администратора безопасности. Выбор ключей шифрования для пользователя

1. Выбранные ключи отобразятся в списке вкладки **Ключи**. При необходимости выберите уровни доступа ключей для чтения и записи. Нажмите **ОК** для создания ключей пользователя или **Отмена** для отказа от их создания (рис. 61).

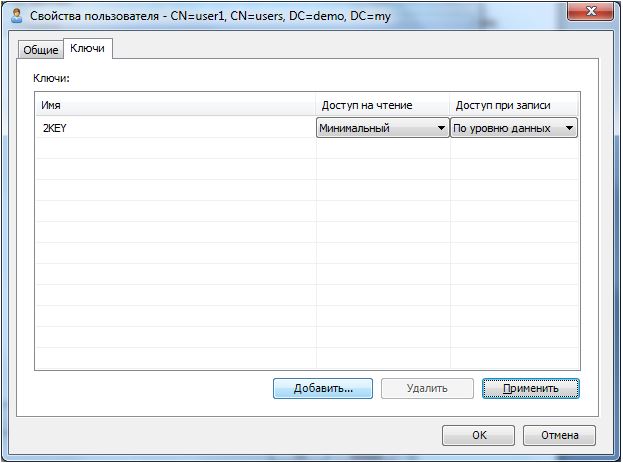


Рис. 61 — Консоль администратора безопасности. Создание ключей пользователя

### Создание ключей пользователя (второй способ)

Данный способ позволяет создать копии одного ключа шифрования для одного или нескольких пользователей. Такой способ может использоваться, например, в случае создания нового ключа шифрования (см. п.14.6.1) и необходимости создания его копий для имеющихся пользователей. Для того чтобы создать ключи пользователя, выполните следующее:

1. В консоли администратора безопасности (рис. 28) раскройте узел **Ключи**.
2. В правой панели выберите ключ шифрования, для которого следует создать пользовательскую копию, и откройте окно его свойств одним из следующих способов:

* дважды нажмите; нажмите правой кнопкой мыши и выберите **Свойства** (рис. 62);
* в меню **Действие** выберите **Свойства**.

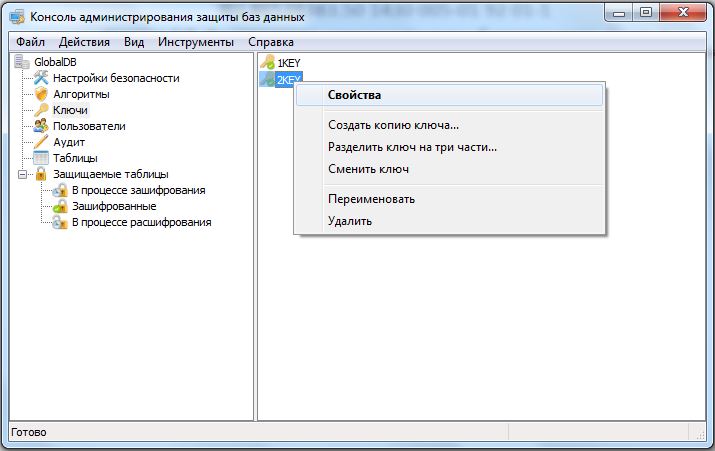


Рис. 62 — Консоль администратора безопасности. Свойства ключа шифрования

1. В открывшемся окне свойств ключа откройте вкладку **Пользователи**.
2. Если вы хотите создать копию выбранного ключа шифрования только для одного пользователя:

* нажмите **Добавить из файла**...;
* в окне выбора файла выберите файл с сертификатом пользователя или ключевым контейнером приложения.

Если вы хотите создать копии выбранного ключа шифрования для нескольких пользователей (приложений):

* нажмите **Добавить из каталога...**;
* выберите папку, содержащую файлы сертификатов пользователей или ключевых контейнеров приложений и нажмите **ОК**.

Если вы хотите создать копии выбранного ключа шифрования для пользователей (приложений), которые были созданы ранее (см. п. 14.8.2):

* нажмите **Добавить из базы данных...**;
* выберите сертификаты пользователей (допускается множественный выбор) и нажмите **ОК** (рис. 63).

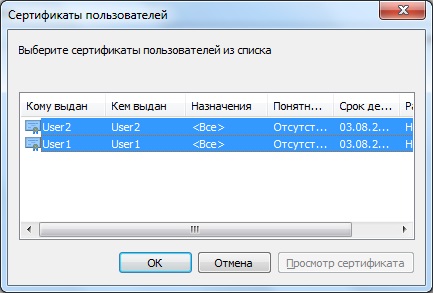


Рис. 63 — Консоль администратора безопасности. Выбор сертификатов из БД

1. Пользователи и/или приложения, для которых созданы копии ключа шифрования, отобразятся во вкладке **Пользователи** окна свойств ключа шифрования (рис. 64).

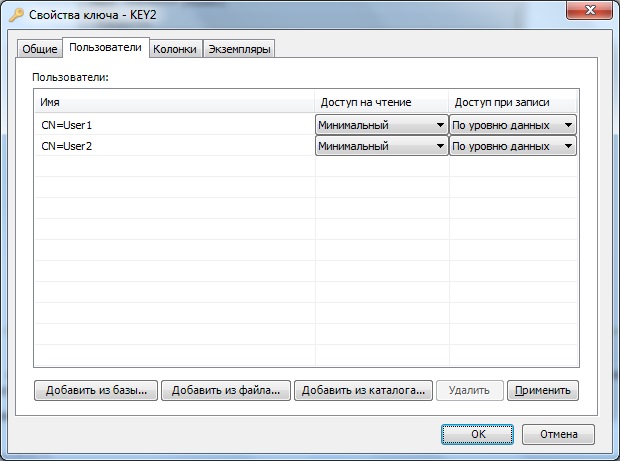


Рис. 64 — Консоль администратора безопасности. Пользователи и приложения, которым предоставлен доступ к ключу шифрования

1. В колонках **Доступ на чтение** и **Доступ на запись** выберите при необходимости соответствующие метки безопасности ключей пользователей.
2. Нажмите **OK**.

Примечания

1. Для штатной работы с защищёнными таблицами пользователь должен иметь USB-токен, смарт-карту или ключевой контейнер на сервере БД с установленными на них сертификатом и парным закрытым ключом. Сертификат должен быть тем же самым сертификатом, который использовался для создания ключа пользователя.
2. В колонках **Доступ на чтение** и **Доступ на запись** отображаются только метки, которые содержатся в справочнике меток. См. раздел 14.5.
3. В случае если пользователь не был заранее создан в Крипто БД (см. п. 14.8), то при создании ключа для сертификата или ключевого контейнера, он будет создан автоматически.

### Удаление ключа пользователей

Действия, описанные ниже, позволяют удалить у одного или нескольких пользователей выбранный ключ шифрования. Удаление ключа пользователей подразумевает изъятие у них прав на использование ключа шифрования, копией которого является удаляемый ключ пользователя, а следовательно, лишение доступа к данным, зашифрованным этим ключом шифрования.

Для того чтобы удалить ключ для пользователей, выполните следующее:

* В консоли администратора безопасности (рис. 28) раскройте папку Ключи.
* В правой панели выберите ключ шифрования, пользователей которого следует удалить, и откройте окно его свойств одним из следующих способов:
* дважды щёлкните; щёлкните правой кнопкой мыши и выберите **Свойства** (рис. 62);
* в меню **Действие** выберите **Свойства**.
* В открывшемся окне свойств ключа откройте вкладку **Пользователи**.
* Выберите пользователей, чьи ключи следует удалить, и нажмите **Удалить**.
* В окне подтверждения убедитесь в том, что вы верно выбрали пользователей. Если это так, нажмите **Да**. В противном случае нажмите **Нет** и вернитесь к шагу 4.

### Удаление ключей пользователя

Действия, описанные ниже, позволяют удалить один или несколько ключей шифрования у выбранного пользователя. Удаление ключа пользователей подразумевает изъятие у него прав на использование ключа шифрования, копией которого является удаляемый ключ пользователя, а следовательно, лишение доступа к данным, зашифрованным этим ключом шифрования.

Для того чтобы удалить ключ для пользователей, выполните следующее:

1. В консоли администратора безопасности (рис. 28) раскройте папку **Пользователи**.
2. В правой панели выберите пользователя, пользовательские копии ключей которого следует удалить, и откройте окно его свойств одним из следующих способов:

* дважды щёлкните; щёлкните правой кнопкой мыши и выберите Свойства (рис. 62);
* в меню Действие выберите Свойства.

1. В открывшемся окне свойств ключа откройте вкладку **Ключи**.
2. Выберите ключи, которые следует удалить, и нажмите **Удалить**.
3. В окне подтверждения убедитесь в том, что вы верно выбрали ключи. Если это так, нажмите **Да**. В противном случае нажмите **Нет** и вернитесь к шагу 4.

## Управление сервером ключей

### Общие сведения о сервере ключей

Штатная работа пользователей и автоматических процессов с зашифрованными данными возможна только после активации сервера ключей, являющегося процедурой обработки ключей, обеспечивающей:

* получение ключей шифрования, зашифрованных на открытом ключе сервера, от сеансов пользователей;
* расшифрование ключей шифрования с помощью закрытого ключа сервера;
* проверку целостности расшифрованных ключей шифрования с использованием подготовленной при создании ключа эталонной пары открытого и зашифрованного текста;
* передачу ключей шифрования в контекст сеансов пользователей;
* установку параметров аудита в контекст сеансов пользователей.

Действия администратора БД и администратора безопасности при работе с сервером ключей указаны в табл. 7.

Табл. 7 — Обязанности администратора БД и администратора безопасности при работе с сервером ключей

|  |  |  |  |
| --- | --- | --- | --- |
| Действие | Исполнитель | Состояния сервера ключей | |
| Исходное | Целевое |
| Активация | Администратор безопасности | выключен | активен |
| Выключение | Администратор безопасности (обычно) или администратор БД (в особых случаях) | активен | выключен |

Активация сервера ключей производится с АРМ администратора безопасности.

При активации сервера ключей автоматически выполняются следующие действия:

* проверка целостности объектов Крипто БД;
* установка настроек аудита;
* установка закрытого ключа сервера ключей.

### Активация сервера ключей

Для того чтобы активировать сервер ключей, на АРМ администратора безопасности выполните следующее.

* Убедитесь в том, что смарт-карта или USB-токен, содержащие закрытый ключ и сертификат администратора безопасности, подключены к АРМ. Если это не так, подключите их.
* В дереве консоли администратора безопасности, соединённой с целевой базой данных (см. выше в разделе 14), выберите Настройки безопасности. В правой панели выберите Сервер ключей.
* Убедитесь в том, что состояние сервера (указано в квадратных скобках) имеет значение "Выключен", далее из контекстного меню (правая кнопка мыши) или из меню Действие выберите Запустить.
* При необходимости в открывшемся окне (рис. 45) введите PIN-код смарт-карты или USB-токена администратора безопасности и нажмите ОК.
* В окне Ввод пароля введите пароль закрытого ключа сервера БД (установленного при создании ключей сервера согласно п. 14.4.1 настоящего документа) в поле Введите пароль и нажмите ОК.
* В случае успешной активации поле Состояние сервера примет значение "Активен" (рис. 65).

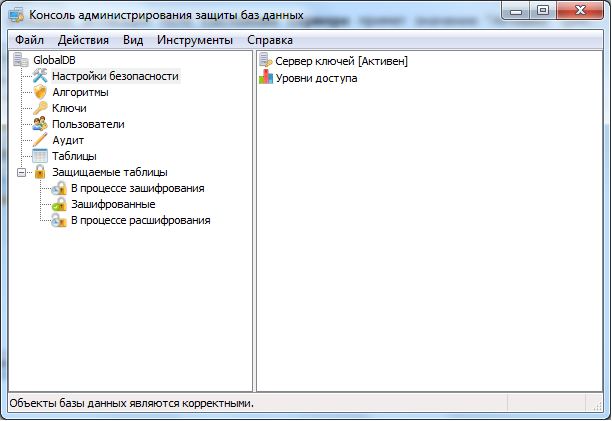


Рис. 65 — Сервер ключей активен

### Выключение сервера ключей

Для того чтобы выключить сервер ключей, выполните следующее.

* Убедитесь в том, что смарт-карта или USB-токен, содержащие закрытый ключ и сертификат администратора безопасности, подключены к АРМ. Если это не так, подключите их.
* В дереве консоли администратора безопасности, соединённой с целевой базой данных (см. выше в разделе 14), выберите **Настройки безопасности**. В правой панели выберите **Сервер ключей**.
* Убедитесь, что состояние сервера имеет значение "Активен". Из контекстного меню (щёлкнув правой кнопки мыши) или из меню **Действие** выберите **Выключить**.
* При необходимости в открывшемся окне (рис. 45) введите PIN-код смарт-карты или USB-токена администратора безопасности и нажмите **ОК**.
* В случае успешного выключения состояние сервера примет значение "Выключен" (рис. 66).

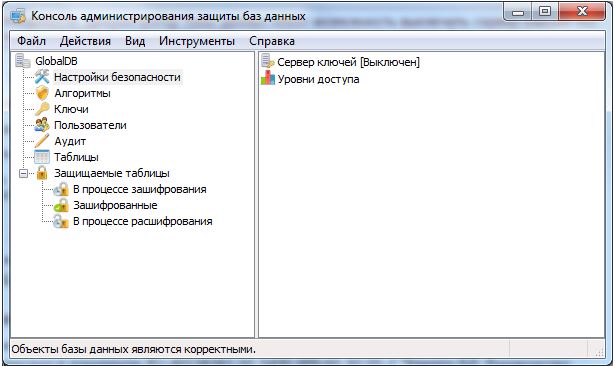


Рис. 66 — Сервер ключей выключен

Примечания

* 1. При необходимости администратор базы данных имеет возможность выключить сервер ключей без участия администратора безопасности, например, при перезагрузке сервера базы данных.

### Рекомендации по работе с сервером ключей

Для предотвращения компрометации закрытого ключа сервера рекомендуется:

* При генерации ключевой пары задавать сложный пароль для шифрования закрытого ключа.
* Обеспечить необходимые меры для сохранения пароля закрытого ключа в тайне.
* Применять средства обеспечения защиты сетевого соединения АРМ администратора безопасности с сервером базы данных.

## Журнал служебных событий

Обращение с журналом служебных событий описано в документе RU.46538383.50 1430 005-01 92 01-2 "Крипто БД. Руководство администратора безопасности. Часть II".

## Контроль целостности

Использование консоли администратора безопасности для выполнения процедур контроля целостности описано в документе RU.46538383.50 1430 005-01 92 01-2 "Крипто БД. Руководство администратора безопасности. Часть II".

# Принципы защиты информации от НСД

Защита информации от НСД в автоматизированной системе обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер. В их числе:

* применение специальных программно-аппаратных средств защиты;
* организация системы контроля безопасности информации;
* физическая охрана АРМ и их средств;
* администрирование информационной безопасности;
* учёт носителей информации;
* сигнализация о попытках нарушения защиты;
* периодическое тестирование технических и программных средств защиты;
* использование сертифицированных программных и технических и средств.

Защита информации от НСД должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе, при проведении ремонтных и регламентных работ. Защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может либо быть периодическим, либо инициироваться по мере необходимости пользователем или контролирующими органами.

В организации, эксплуатирующей СКЗИ "Крипто БД 2.0", должна быть разработана инструкция по защите от НСД к системе, базирующаяся на настоящем документе, руководящих документах ФСТЭК и ФСБ, действующих нормативных документов самой эксплуатирующей организации.

В организации должно быть выделено специальное должностное лицо — администратор безопасности, функции которого должны заключаться в выполнении процедур установки и удаления ПО, настройки системного окружения, установки, настройки, обслуживания и обеспечения функционирования средств защиты, а также разработки рекомендаций и регламентов для администраторов баз данных и пользователей. Администратор безопасности должен иметь возможность доступа ко всей информации, обрабатываемой на своём рабочем месте. Каждый исполнитель работ как пользователь базы данных, содержащей защищённую информацию, должен быть зарегистрирован у администратора службы безопасности. При осуществлении доступа в глобальные сети передачи данных непосредственно с рабочих мест, оснащённых СКЗИ "Крипто БД 2.0", должны быть приняты меры, исключающие возможность воздействия нарушителя на СКЗИ по каналам связи, выходящим за пределы контролируемой зоны.

# Обеспечение безопасности функционирования рабочих мест и серверов со встроенными средствами криптографической защиты

Настоящий раздел посвящён рекомендациям по организационно-техническим мерам защиты для обеспечения безопасности СВТ (АРМ пользователей и серверы баз данных) с установленной СКЗИ "Крипто БД 2.0".

* Использование шифровальных средств для криптографической защиты информации подлежит лицензированию в соответствии с действующим законодательством РФ.
* Рабочие места пользователей и серверы баз данных, на которые установлено СКЗИ "Крипто БД 2.0", должны быть аттестованы комиссией, специально формируемой для аттестации СВТ. Результаты аттестации отражаются в акте о готовности к работе (см. Приложение А).
* Доступ к рабочим местам с установленным СКЗИ "Крипто БД 2.0" предоставляется только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на программное обеспечение, использующее СКЗИ "Крипто БД 2.0". Администратор безопасности должен ознакомить каждого пользователя, использующего СКЗИ "Крипто БД 2.0", с правилами пользования, а также иными нормативными документами.

1. Должностные инструкции администратора безопасности (его заместителя) и ответственного исполнителя должны учитывать рекомендации, приведённые в настоящем разделе.
2. Следует запретить:

* внесение изменений в программное обеспечение СКЗИ "Крипто БД 2.0";
* изменение настроек, установленных программой установки СКЗИ "Крипто БД 2.0" или администратором безопасности;
* осуществление не санкционированного администратором безопасности копирования ключей шифрования на ключевые носители;
* при генерации ключей шифрования использование синхропосылок, вырабатываемых не средствами сертифицированного СКЗИ;
* несанкционированное копирование ключевых носителей;
* разглашение содержимого ключевых носителей и передачу самих носителей лицам, к ним не допущенным;
* использование ключевых носителей в режимах, не предусмотренных правилами пользования СКЗИ "Крипто БД 2.0";
* запись на ключевые носители посторонней информации;
* использование бывших в работе ключевых носителей для записи новой информации без предварительного уничтожения на них ключевой информации (форматирования ключевого носителя);
* подключение к АРМ или серверному оборудованию дополнительных устройств и соединителей, не предусмотренные штатной комплектацией;
* обработку на АРМ и серверах баз данных, оснащённых СКЗИ "Крипто БД 2.0", информации, содержащей государственную тайну;
* несанкционированное вскрытие системных блоков АРМ, серверного оборудования.

1. На технических средствах (серверах баз данных и АРМ), оснащённых СКЗИ "Крипто БД 2.0", программное обеспечение должно использоваться строго по лицензии фирм-производителей.
2. Не допускается установка на АРМ и серверы программного обеспечения со встроенными средствами разработки и отладки программ. Если средства отладки приложений необходимы для технологических потребностей пользователя, то их использование должно быть санкционировано администратором безопасности. В любом случае запрещается использовать эти средства для просмотра и редактирования кода и памяти приложений, использующих СКЗИ "Крипто БД 2.0".
3. Необходимо исключить попадание в систему программ, позволяющих, пользуясь ошибками приложений или ОС, получать привилегии администратора.
4. Пользователь должен запускать только те приложения, использование которых разрешено администратором безопасности.
5. Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых установлены технические средства СКЗИ "Крипто БД 2.0", лиц, не допущенных к работе в указанных помещениях.
6. Должно быть запрещено бесконтрольное оставление СВТ, на которых эксплуатируется СКЗИ "Крипто БД 2.0", после ввода ключевой информации. Для АРМ пользователей и администратора безопасности при кратковременном перерыве в работе рекомендуется производить автоматическое блокирование АРМ, с последующим вводом пароля либо PIN-кода для возобновления работы.
7. Пароли, назначаемые пользователям, должны отвечать требованиям соответствующих инструкций и нормативных документов, а также критериям, приведённым в разделе 16.
8. Администратором безопасности должно быть проведено опечатывание системных блоков АРМ пользователей и серверного оборудования с установленным СКЗИ "Крипто БД 2.0", исключающее возможность несанкционированного изменения аппаратной части.
9. Помещения, в которых устанавливаются СВТ сервера БД, после проведения работ администраторами СУБД и администраторами безопасности должны закрываться и опечатываться.
10. Перед каждым включением рабочей станции с установленным СКЗИ "Крипто БД 2.0" необходимо проверять сохранность печатей системного блока и разъёмов рабочей станции. Также следует проверять сохранность печатей на помещениях с серверным оборудованием.
11. Из состава системы должно быть исключено всё оборудование, которое может создавать угрозу безопасности ОС или серверу БД. Также следует избегать использования любых нестандартных аппаратных средств, имеющих возможность влиять на нормальный ход работы компьютера, ОС или СУБД.
12. При использовании СКЗИ "Крипто БД 2.0" на АРМ, подключённых к общедоступным сетям связи, должны быть предприняты дополнительные меры, исключающие возможность несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей.
13. В BIOS АРМ определяются установки, исключающие возможность загрузки операционной системы, отличной от установленной на жёстком диске: отключается возможность загрузки с гибкого диска, привода лазерных дисков и прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Не применяются ПЭВМ с BIOS, исключающим возможность отключения сетевой загрузки ОС.
14. Средствами BIOS должна быть исключена возможность отключения пользователями устройств PCI или PCI-E при использовании ПАК защиты от НСД, устанавливаемых в указанные разъёмы.
15. Вход в BIOS ПЭВМ должен быть защищён паролем, к качеству которого предъявляются требования, изложенные в разделе 17. Пароль для входа в BIOS должен быть известен только администратору и быть отличным от пароля администратора для входа в ОС (в случае использования пароля для интерактивного входа в систему).
16. Средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты.
17. Администратор безопасности должен периодически (не реже 1 раза в 2 месяца) проводить контроль целостности и легальности установленных копий ПО "Крипто БД 2.0" на всех АРМ и серверах БД с помощью консоли администратора безопасности.
18. В случае обнаружения незарегистрированных программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках или серверном оборудовании работа на АРМ пользователей должна быть прекращена. По данному факту должно быть проведено служебное расследование комиссией в составе представителей служб информационной безопасности организации-владельца, где произошло нарушение, и организованы работы по анализу и ликвидации негативных последствий данного нарушения.
19. Рекомендуется использовать дополнительные средства контроля целостности программного обеспечения, входящего в состав СКЗИ "Крипто БД 2.0", самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ, при загрузке ОС.
20. Рекомендуется применение сертифицированных средств обеспечения защиты сетевого соединения АРМ пользователей с сервером базы данных.
21. Не рекомендуется:

* подключение АРМ администратора безопасности к сетям общего пользования;
* использование в помещении, где размещены средства СКЗИ, радиотелефонов и другой радиопередающей аппаратуры.

# Критерии качества паролей

Все пароли, использующиеся в СКЗИ "Крипто БД 2.0" и в среде его функционирования должны удовлетворять следующим критериям:

* длина — не менее 8 символов;
* пароль должен содержать:
* не менее одной заглавной буквы;
* не менее одной строчной буквы;
* не менее одной цифры;
* не менее одного символа, не являющегося ни буквой, ни цифрой.

# Нештатные ситуации при эксплуатации СКЗИ

Табл. 8 — Действия персонала в нештатных ситуациях

| Нештатная ситуация | Действия персонала |
| --- | --- |
| Эвакуация, угроза нападения, взрыва и т.п., стихийные бедствия, аварии общего характера. | 1. Остановить все АРМ. 2. Персонал, имеющий доступ к ключам, обязан сдать все имеющиеся у него в наличии аппаратные хранилища ключей администратору безопасности. С консоли управления администратор безопасности останавливает работу сервера ключей (см. п. 14.10.2). 3. Администратор безопасности упаковывает все аппаратные хранилища ключей пользователей в опечатываемый контейнер, который выносит в безопасное помещение или здание. Опечатанный контейнер должен находиться под охраной до окончания действия нештатной ситуации и восстановления нормальной работы аппаратных и программных средств СКЗИ. 4. Администратор безопасности оповещает по телефонным каналам общего пользования всех пользователей о приостановке работы системы. 5. В случае наступления события, повлекшего за собой долговременный выход из строя аппаратных средств СКЗИ, администратор безопасности уничтожает всю информацию с аппаратных носителей, находящихся в контейнере. |
| Компрометация, утеря, выход из строя аппаратного хранилища ключей пользователя. | Порядок действий при компрометации ключей описан в п. 10.7.3. |
| Отказы и сбои в работе аппаратной части АРМ пользователей, сервера базы данных с установленным СКЗИ. | Необходимо остановить работу, локализовать неисправность и произвести ремонт в установленном порядке. При необходимости переустановить СКЗИ на АРМ пользователя или сервере базы данных. |
| Отказы и сбои в работе средств защиты от НСД. | При отказах и сбоях в работе средств защиты от НСД администратор безопасности, должен восстановить работоспособность средств защиты от НСД, при необходимости переустановить программно-аппаратные средства НСД. |
| Отказы и сбои в работе программных средств вследствие не выявленных ранее ошибок в программном обеспечении. | При отказах и сбоях в работе программных средств вследствие ранее не выявленных ошибок в программном обеспечении, необходимо остановить работу, локализовать по возможности причину отказов и сбоев и вызвать разработчика данного ПО или его представителя для устранения причин, вызывающих отказы и сбои. |
| Отказы в работе программных средств вследствие случайного или умышленного их повреждения. | При отказах в работе программных средств вследствие случайного или умышленного их повреждения лицо, ответственное за безопасность функционирования программных и аппаратных средств, обязано произвести служебное расследование по данному факту с целью установления причины отказа и восстановления правильной работы программных средств в установленном порядке. |
| Отказы в работе программных средств вследствие ошибок оператора. | При отказах в работе программных средств, вследствие ошибок оператора последний сообщает о данном факте лицу, ответственному за безопасность функционирования программных и аппаратных средств. Лицо, ответственное за безопасность функционирования программных и аппаратных средств, даёт соответствующие указания обслуживающему персоналу по восстановлению правильной работы программных средств в установленном порядке. |

Все нештатные ситуации должны отражаться в журнале пользователя "Крипто БД 2.0" (см. подраздел 10.8).

# Литература

* Федеральный закон № 149-Ф3 от 27.07.06 г. "Об информации, информационных технологиях и о защите информации".
* Федеральный закон № 152-ФЗ от 27.07.06 г. "О персональных данных".
* ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.
* ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
* ГОСТ Р 34.10-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
* ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
* ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования.
* ГОСТ Р 50739-95. Государственный стандарт Российской Федерации. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.
* ГОСТ Р 1.0-92. Государственная система стандартизации Российской Федерации. Основные положения.
* ГОСТ 16487-83. Делопроизводство и архивное дело. Термины и определения.
* ГОСТ Р 50922-96. Государственный стандарт Российской Федерации. Защита информации. Основные термины и определения.
* Толковый словарь по информатике. - М.: Финансы и статистика, 1991.
* Гостехкомиссия России. Руководящий документ. Защита от НСД к информации. Термины и определения. - М.: Воениздат, 1992.
* Закон РФ № 2446-1 от 05.03.92 г. "О безопасности" (редакция от 02.03.2007 г.).
* Положение о государственном лицензировании деятельности в области защиты информации. Утверждено Решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации № 10 от 27 апреля 1994 г. (с дополнениями от 24 июня 1997 года № 60).
* Гостехкомиссия России. Концепция защиты информации в системах ее обработки, 1995.
* Халянин Д.В., Ярочкин В.И. Основы защиты промышленной и коммерческой информации. Термины и определения: Словарь / ИПКИР. - М., 1994.
* Терминология в области защиты информации: Справочник / ВНИИстандарт, 1993.
* Закон РФ № 5485-1 от 21.07.93 г. "О государственной тайне" (в редакции от 01.12.2007 г.).
* Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации. Москва, 1992 г.
* Федеральный закон № 184-ФЗ от 27.12.02 г. “О техническом регулировании”.
* Гражданский кодекс Российской Федерации № 51-ФЗ. Ч.1.
* Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. Москва, 1992 г.
* RFC 4357. Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms.
* RFC 4490. Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS).
* RFC 5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
* ГОСТ Р 34.12-2015 "Информационная технология. Криптографическая защита информации. Блочные шифры".
* ГОСТ Р 34.13-2015 "Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров".
* ТК 026 "Системы обработки информации. Защита криптографическая. Использование криптографических алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012".
* ТК 026 "Системы обработки информации. Защита криптографическая. Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических  сообщениях формата CMS".
* ТК 026 "Парольная защита с использованием алгоритмов ГОСТ".
* ТК 026 "Транспортный ключевой контейнер".
* Microsoft Knowledge Base, Article 324750: HOW TO: Assign Software to a Specific Group By Using a Group Policy in the Windows Server 2003 Family.
* Microsoft Knowledge Base, Article 816102: HOW TO: Use Group Policy to remotely install software in Windows Server 2003 and in Windows Server 2008.

# Приложение А. Акт о готовности к работе

**УТВЕРЖДАЮ**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование учреждения)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (Ф.И.О.)

АКТ

о готовности к работе \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование учреждения) (наименование изделий)

"\_\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_г.

Комиссия в составе председателя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ и членов комиссии (должность) (Ф.И.О.)

назначенная \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ составила настоящий акт о том, что помещение

эксплуатирующего органа \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, размещение \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, оборудование , хранилища ключевых носителей, охрана помещений и подготовленность сотрудников к обслуживанию \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

соответствуют: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ГОСТ, инструкция, руководящие документы, правила пользования и т.п.)

Комиссия отмечает, что установка ПО вышеупомянутых изделий проведены в соответствии с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

инструкции

Вывод:

комиссия считает, объект\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ отвечает требованиям

название объекта

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

название инструкции

по обеспечению безопасности связи по уровню \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ и может быть введён в действие.

Председатель:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись)

(Ф.И.О)

Члены комиссии

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись)

(Ф.И.О)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись)

(Ф.И.О)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись)

(Ф.И.О)

**М.П.**

# Приложение Б. Пример журнала пользователей СКЗИ "Крипто БД 2.0"

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| №  п/п | Дата | Вре­мя | Объект или поль­зо­ва­тель | Тип со­бы­тия | До­пол­ни­тельные све­де­ния | Ф.И.О. ад­ми­ни­стра­то­ра безопас­нос­ти | Подпись ад­ми­ни­стра­то­ра безопас­нос­ти |
| 1 | 01.11.06 | 11:00 | Сервер БД | Создание ключа шифрования | Ключ К122 | Иванов И. И. |  |
| 2 | 02.11.06 | 11:15 | Петров П.П. /  Пользователь АРМ "Склад" | Создание копии ключа шифрования | Ключ К122 | Иванов И. И. |  |
| 3 | 03.11.06 | 12:00 | Схема HR, таблица EMPLOYEES, колонка PHONE\_NUMBER | За­шиф­ро­ва­ние | Ключ К122 | Иванов И. И. |  |
| 4 | 01.02.08 | 12:45 | Сервер БД | Смена ключа шифрования | Ключ К122 | Иванов И. И. |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

# Приложение В. Перечень и обозначения алгоритмов шифрования

В справочнике алгоритмов наименования алгоритмов представлены в виде условных обозначений следующего формата:

**<Алгоритм>-<Таблица замен>|<Размер блока>-<Режим>-<Дополнительно>-<MAC>**, где:

**<Алгоритм>** - стандарт алгоритма, одно из значений:

* **ГОСТ28147** - соответствует [4];
* **ГОСТР3412** - соответствует [27].

**<Таблица замен>** - условное обозначение таблицы замен (только для **ГОСТ28174**). Одно из значений:

* **A** - таблица замен A. Соответствует описанию в [24];
* **B** - таблица замен B. Соответствует описанию в [24];
* **C** - таблица замен C. Соответствует описанию в [24];
* **Z** - таблица замен Z. Соответствует описанию в [28].

**<Размер блока>** - размер блока алгоритма в битах (только для **ГОСТР3412**). Одно из значений:

* **64** - для алгоритма [27] ("Магма");
* **128** - для алгоритма [27] ("Кузнечик").

**<Режим>** - режим работы алгоритма в соответствие с [4],[28]. Одно из значений:

* **ECB** - режим простой замены;
* **CFB** - режим сцепления блоков с обратной связью;
* **CTR** - режим гаммирования (счётчика).

**<Дополнительно>** - режим диверсификации ключа ключа. Необязательный параметр. Допустимы значения:

* **UKM** - диверсификации ключа согласно [24].

**<MAC>** - дополнительное вычисление и проверка имитовставки. Необязательный параметр. Допустимы значения:

* **MAC** - допонительное вычисление/проверка имитовставки.