УТВЕРЖДЕНА
Приказом Закрытого акционерного общества
ВТБ Специализированный депозитарий
от 24 февраля 2011 г. № 19

И Н С Т Р У К Ц И Я
по обеспечению безопасности эксплуатации средств криптографической защиты информации в системе электронного документооборота ЗАО ВТБ Специализированный депозитарий

СОДЕРЖАНИЕ

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. В настоящей Инструкции по обеспечению безопасности эксплуатации средств криптографической защиты информации в системе электронного документооборота ЗАО ВТБ Специализированный депозитарий (далее – Инструкция) применяются следующие термины и определения:

Администратор безопасности **–** должностное лицо Организатора СЭД, обеспечивающее эксплуатацию СКЗИ и управление криптографическими ключами.

Безопасность эксплуатации СКЗИ – совокупность мер управления и контроля, защищающая СКЗИ и криптографические ключи от несанкционированного (умышленного или случайного) их раскрытия, модификации, разрушения или использования.

Договор – Договор об электронном документообороте или Договор об обеспечении транзита электронных документов.

Организатор СЭД – Закрытое акционерное общество ВТБ Специализированный депозитарий.

Ответственный за эксплуатацию СКЗИ **–** работник Участника СЭД, осуществляющий организацию и обеспечение работ по техническому обслуживанию СКЗИ и управление криптографическими ключами Участника СЭД.

Пользователь – работник Участника СЭД, который использует СКЗИ для обеспечения электронного документооборота.

Правила ЭДО **–** правила, определяющие условия, порядок организации и обеспечения электронного документооборота, а также порядок организации использования СКЗИ и сертификатов ключей подписи.

ПЭВМ – персональная электронно-вычислительная машина (персональный компьютер).

Система электронного документооборота (СЭД) **–** организационно-техническая система, представляющая собой совокупность нормативного, программного, информационного и технического обеспечения Организатора СЭД.

Средства криптографической защиты информации (СКЗИ) – совокупность программно-технических средств, обеспечивающих применение ЭЦП и/или шифрования при осуществлении электронного документооборота.

Участник СЭД – юридическое лицо, которое заключило с Организатором СЭД Договор.

Электронный документ (ЭД) – документ, в котором информация, имеющая смысл для Участников СЭД, представлена в электронно-цифровой форме в установленном Правилами ЭДО формате. Электронный документ подписан ЭЦП и может быть представлен в форме документа с использованием программного обеспечения, определенного Правилами ЭДО. Электронный документ, оформленный в соответствии с Правилами ЭДО, имеет юридическую силу для Участников СЭД.

Электронный документооборот (ЭДО) – обмен электронными документами в соответствии с Правилами ЭДО.

Электронная цифровая подпись (ЭЦП) – реквизит ЭД, предназначенный для защиты данного ЭД от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в ЭД.

1.2. Остальные термины и определения, используемые в настоящей Инструкции, должны пониматься в соответствии с законодательством Российской Федерации и Правилами электронного документооборота.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящая Инструкция определяет порядок учета, хранения и использования СКЗИ и криптографических ключей, а также порядок изготовления, смены, уничтожения и компрометации криптографических ключей в целях обеспечения безопасности эксплуатации СКЗИ.

2.2. Настоящая Инструкция разработана на основе законодательства Российской Федерации, иных правовых актов, а также:

Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом ФСБ России от 9 февраля 2005 г. № 66;

Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом ФАПСИ от 13 июня 2001 г. № 152.

2.3. Участник СЭД с учетом особенностей своей деятельности может разрабатывать не противоречащие настоящей Инструкции организационно-распорядительные и методические документы, уточняющие порядок работы с СКЗИ и криптографическими ключами.

2.4. Организатор СЭД, имеет все необходимые лицензии ФСБ России на деятельность по использованию СКЗИ (шифровальных средств) в СЭД. С лицензиями ФСБ России, выданными Организатору СЭД, можно ознакомиться на Web-сайте по адресу в сети Интернет http://www.vtbsd.ru.

На Участника СЭД, использующего СКЗИ в СЭД, распространяется действие лицензий ФСБ России, полученных Организатором СЭД, и ему не требуется получения отдельных лицензий.

2.5. В СЭД используются сертифицированные ФСБ России СКЗИ, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну, при обеспечении безопасности информации по уровню «КС1». Организатор СЭД предоставляет Участникам СЭД СКЗИ во временное пользование на период действия Договора ***только*** для использования в СЭД.

2.6. Для организации и обеспечения работ по техническому обслуживанию СКЗИ и управления криптографическими ключами приказом руководителя организации Участника СЭД (Приложение № 1 к настоящей Инструкции) назначается Ответственный за эксплуатацию СКЗИ.

Ответственный за эксплуатацию СКЗИ осуществляет:

поэкземплярный учет предоставленных Участнику СЭД СКЗИ, эксплуатационной и технической документации к ним;

учет Пользователей СКЗИ Участника СЭД;

контроль за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией на СКЗИ и настоящей Инструкцией;

расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации;

разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

2.7. Пользователи СКЗИ назначаются приказом руководителя Участника СЭД (Приложение № 2 к настоящей Инструкции).

Пользователь СКЗИ обязан:

не разглашать конфиденциальную информацию, к которой допущен, рубежи ее защиты, в том числе сведения о криптографических ключах;

соблюдать требования к обеспечению безопасности конфиденциальной информации при использовании СКЗИ;

сдать СКЗИ, эксплуатационную и техническую документацию к ним, криптографические ключи в соответствии с порядком, установленным настоящей Инструкцией, при прекращении использования СКЗИ;

незамедлительно уведомлять Ответственного за эксплуатацию СКЗИ о фактах утраты или недостачи СКЗИ, криптографических ключей, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

2.8. Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения.

Обучение Пользователей правилам работы с СКЗИ осуществляет Ответственный за эксплуатацию СКЗИ. Ответственный за эксплуатацию СКЗИ должен иметь соответствующий документ о квалификации в области эксплуатации СКЗИ.

2.9. Текущий контроль, обеспечение функционирования и безопасности СКЗИ возлагается на Ответственного за эксплуатацию СКЗИ.

2.10. Ответственный за эксплуатацию СКЗИ и Пользователи Участника СЭД должны быть ознакомлены с настоящей Инструкцией под расписку.

3. УЧЕТ И ХРАНЕНИЕ СКЗИ И КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

3.1. СКЗИ, эксплуатационная и техническая документация к ним, криптографические ключи подлежат поэкземплярному учету.

3.2. Поэкземплярный учет ведет Ответственный за эксплуатацию СКЗИ Участника СЭД в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал), форма которого приведена в Приложении № 3 к настоящей Инструкции. При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатная эксплуатация. Если аппаратные или аппаратно-программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно с соответствующими аппаратными средствами.

3.3. Единицей поэкземплярного учета криптографических ключей считается отчуждаемый ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи криптографических ключей, то его каждый раз следует регистрировать отдельно.

3.4. Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, криптографических ключей должны быть выданы под расписку в Журнале Пользователям СКЗИ, несущим персональную ответственность за их сохранность.

3.5. Дистрибутивы СКЗИ на магнитных носителях, эксплуатационная и техническая документация к СКЗИ хранятся у Ответственного за эксплуатацию СКЗИ. Криптографические ключи хранятся у Пользователей СКЗИ. Хранение осуществляется в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.6. Пользователи СКЗИ могут осуществлять хранение рабочих и резервных криптографических ключей, предназначенных для применения в случае неработоспособности рабочих криптографических ключей. Резервные криптографические ключи могут также находится на хранении у Ответственного за эксплуатацию СКЗИ.

3.7. На ключевые носители с изготовленными криптографическими ключами наклеиваются наклейки, содержащие надписи:

на один ключевой носитель - «Рабочий»;

на другой ключевой носитель - «Резервный».

3.8. Ключевой носитель с наклейкой «Резервный» помещается в конверт и опечатывается Пользователем и Ответственным за эксплуатацию СКЗИ.

3.9. Полученные рабочие и резервные криптографические ключи Пользователь обязан учесть в Описи криптографических ключей Пользователя СКЗИ (Приложение № 4 к настоящей Инструкции). Резервные криптографические ключи могут находиться на хранении у Ответственного за эксплуатацию СКЗИ.

3.10. Ключевые носители с неработоспособными криптографическими ключами Ответственный за эксплуатацию СКЗИ принимает от Пользователя под роспись в Описи криптографических ключей Пользователя СКЗИ и в Журнале поэкземплярного учета. Неработоспособные ключевые носители подлежат уничтожению.

3.11. При необходимости замены наклейки на ключевом носителе (стирание надписи реквизитов) Пользователь передает его Ответственному за эксплуатацию СКЗИ, который в присутствии Пользователя снимает старую наклейку и приклеивает новую наклейку с такими же учетными реквизитами.

3.12. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

3.13. СКЗИ и криптографические ключи могут доставляться Участнику СЭД специальной (фельдъегерской) связью или курьером Участника СЭД, имеющего доверенность, подписанную руководителем организации Участника СЭД, на право получения СКЗИ, при соблюдении мер, исключающих бесконтрольный доступ к СКЗИ и криптографическим ключам во время доставки.

3.14. Для пересылки СКЗИ и криптографические ключи помещаются в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. Криптографические ключи пересылают в отдельном пакете с пометкой «Лично». Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения целостности упаковок и оттисков печати.

3.15. Для пересылки СКЗИ, эксплуатационной и технической документации к ним, криптографических ключей составляется Акт приема-передачи (Опись) документов, в котором указывается: что посылается и в каком количестве, учетные номера СКЗИ, криптографических ключей или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Акт приема-передачи (Опись) документов вкладывается в упаковку.

3.16. Полученную Участником СЭД упаковку вскрывает только лицо, для которого она предназначена. Если содержимое полученной упаковки не соответствует указанному в Акте приема-передачи (Описи) документов или сама упаковка и оттиск печати – их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то Участник СЭД должен составить акт, который высылается Организатору СЭД. Полученные с такими отправлениями СКЗИ и криптографические ключи до получения указаний от Организатора СЭД применять не разрешается.

3.17. При обнаружении бракованных криптографических ключей ключевой носитель с такими ключами следует возвратить Организатору СЭД для установления

причин происшедшего и их устранения в дальнейшем. Организатор СЭД в этом случае направляет Участнику СЭД новые криптографические ключи.

3.18. Ключевые носители совместно с Описью криптографических ключей должны храниться Пользователем в сейфе (металлическом шкафу), как правило, в отдельной ячейке. В исключительных случаях допускается хранить ключевые носители и Опись криптографических ключей совместно с другими документами, при этом ключевые носители и Опись криптографических ключей должны быть помещены в отдельную папку.

3.19. При отсутствии у Пользователя СКЗИ сейфа (металлического шкафа) ключевые носители в опечатанном пенале (тубусе) по окончании рабочего дня должны сдаваться назначенному работнику Участника СЭД по Реестру передачи криптографических ключей (Приложение № 5 к настоящей Инструкции).

4. ИСПОЛЬЗОВАНИЕ СКЗИ И КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

4.1. В СЭД СКЗИ и криптографические ключи используются для обеспечения конфиденциальности, авторства и целостности электронных документов.

4.2. Конфиденциальность электронных документов обеспечивается путем их шифрования. Авторство и целостность электронных документов обеспечивается путем создания в документе ЭЦП Пользователя.

4.3. В СЭД используются СКЗИ с открытым распределением ключей.

4.4. Электронный документ может быть подписан ЭЦП с использованием только того закрытого ключа ЭЦП, для которого Организатором СЭД выдан сертификат ключа подписи Пользователя с областью действия «Система электронного документооборота ЗАО ВТБ Специализированный депозитарий».

4.5. Для зашифрования электронного документа Пользователь использует свой собственный закрытый криптографический ключ и открытый криптографический ключ, соответствующий действующему закрытому криптографическому ключу получателя документа.

Открытый криптографический ключ содержится в сертификате ключа подписи, который выдается Организатором СЭД Пользователю в электронной форме и на бумажном носителе.

4.6. Проверка подлинности ЭЦП электронного документа осуществляется Пользователем с использованием открытого криптографического ключа отправителя документа.

4.7. Расшифрование электронного документа осуществляется с использованием закрытого криптографического ключа Пользователя и открытого криптографического ключа отправителя документа.

4.8. Пользователь не может подписать электронный документ своей ЭЦП или выполнить его зашифрование, если истек срок действия закрытых криптографических ключей. Также Пользователь не может проверить ЭЦП электронного документа или произвести его расшифрование в случае истечения срока действия сертификата ключа подписи, необходимого для выполнения соответствующей операции.

4.9. Реализованные в СКЗИ алгоритмы шифрования и электронной цифровой подписи гарантируют невозможность восстановления закрытых криптографических ключей отправителя по его открытым ключам.

4.10. Для обеспечения контроля доступа к СКЗИ системный блок ПЭВМ опечатывается Ответственным за эксплуатацию СКЗИ. Системный блок ПЭВМ может устанавливаться в специальном опечатываемом шкафу.

4.11. Пользователь должен периодически (ежедневно) проверять сохранность оборудования и целостность печатей на ПЭВМ. В случае обнаружения «посторонних» (не

зарегистрированных) программ или выявления факта повреждения печати на системном блоке ПЭВМ ***работа должна быть прекращена***. По данному факту проводится служебное расследование, и осуществляются работы по анализу и ликвидации последствий данного нарушения.

4.12. При выявлении сбоев или отказов Пользователь обязан сообщить о факте их возникновения Ответственному за эксплуатацию СКЗИ и предоставить ему носители криптографических ключей для проверки их работоспособности. Проверку работоспособности носителей криптографических ключей Ответственный за эксплуатацию СКЗИ выполняет в присутствии Пользователя.

4.13. В случае, если рабочие криптографические ключи потеряли работоспособность, то по просьбе Пользователя Ответственный за эксплуатацию СКЗИ, вскрывает конверт с резервными криптографическими ключами, делает копию ключевого носителя, используя резервные криптографические ключи, помещает резервные криптографические ключи в конверт, а на новый ключевой носитель наклеивает наклейку с надписью «Рабочий».

4.14. В экстренных случаях, не терпящих отлагательства, вскрытие конверта с резервными криптографическими ключами может осуществляться Пользователем самостоятельно с последующим уведомлением Ответственного за эксплуатацию СКЗИ о факте вскрытия конверта с криптографическими ключами. На конверте делается запись о вскрытии с указанием даты и времени вскрытия конверта и подписью Пользователя. Вскрытый конверт вместе с неработоспособными криптографическими ключами сдаются Ответственному за эксплуатацию СКЗИ.

4.15. Вскрытие системного блока ПЭВМ, на которой установлено СКЗИ, для проведения ремонта или технического обслуживания должно осуществляться в присутствии Ответственного за эксплуатацию СКЗИ.

4.16. Пользователю ***ЗАПРЕЩАЕТСЯ:***

осуществлять несанкционированное копирование криптографических ключей;

использовать ключевые носители для работы на других рабочих местах или для шифрования и подписи электронных документов, не относящейся к работе в СЭД;

разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;

вставлять носители криптографических ключей в устройства считывания в режимах, не предусмотренных штатным режимом работы СКЗИ, а также в устройства считывания других ПЭВМ;

записывать на носители с криптографическими ключами постороннюю информацию;

подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные в штатной комплектации;

работать на ПЭВМ, если во время ее начальной загрузки не проходят встроенные тесты, предусмотренные в ПЭВМ;

вносить какие-либо изменения в программное обеспечение СКЗИ;

использовать бывшие в работе ключевые носители для записи новых криптографических ключей.

5. ИЗГОТОВЛЕНИЕ И ПЛАНОВАЯ СМЕНА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

5.1. Изготовление криптографических ключей может производиться:

Администратором безопасности в присутствии Пользователя;

Администратором безопасности без присутствия Пользователя;

Пользователем собственноручно.

5.2. Криптографические ключи изготавливаются на отчуждаемый ключевой носитель (дискету, ruToken, EToken и др.) в соответствии с эксплуатационно-технической документацией на СКЗИ и требованиями безопасности, установленными настоящей Инструкцией.

5.3. При самостоятельном изготовлении криптографического ключа создается запрос на сертификат ключа подписи, который передается Администратору безопасности в электронной форме. После выпуска сертификата ключа подписи Администратор безопасности передает его Пользователю в электронной форме и бумажном носителе в соответствии с определенным Правилами ЭДО порядком.

5.4. Сертификат ключа подписи на бумажном носителе изготавливается в двух экземплярах, один из которых после подписания собственноручными подписями Пользователя и руководителя организации Участника СЭД и заверения оттиском печати организации Участника СЭД подлежит возвращению Администратору безопасности.

5.5. В целях обеспечения непрерывности электронного документооборота плановую смену криптографических ключей следует производить заблаговременно (за 2 (два) месяца до окончания скока действия закрытых криптографических ключей). Использование закрытых криптографических ключей производится после получения от Организатора СЭД уведомления о вводе в действия сертификатов ключей подписи, соответствующих этим ключам.

5.6. Переход на новые криптографические ключи и установку новых сертификатов ключей подписи Пользователь выполняет самостоятельно в соответствии с эксплуатационной документацией на СКЗИ. Переход на новые криптографические ключи осуществляется в сроки, указанные в сертификате ключа подписи.

5.7. При замене криптографических ключей Удостоверяющего центра ОАО Банк ВТБ или других Участников СЭД Пользователь самостоятельно обязан обновить справочники сертификатов ключей подписи. Обновление справочников сертификатов ключей подписи производится путем добавления новых сертификатов ключей подписи из сетевых справочников сертификатов ключей подписи либо из файлов, содержащих сертификаты ключей подписи, размещаемых в сети Интернет или рассылаемых по электронной почте. Обновление справочников сертификатов ключей подписи осуществляется в соответствии с эксплуатационной документацией на СКЗИ.

6. ДЕЙСТВИЯ ПРИ КОМПРОМЕТАЦИИ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

6.1. К обстоятельствам, указывающим на возможную компрометацию криптографических ключей, но не ограничивающим их, относятся следующие:

потеря ключевых носителей с рабочими и/или резервными криптографическими ключами;

потеря ключевых носителей с рабочими и/или резервными криптографическими ключами с последующим их обнаружением;

увольнение работников, имевших доступ к рабочим и/или резервным криптографическим ключам;

возникновение подозрений относительно утечки информации или ее искажения;

нарушение целостности печатей на сейфах (металлических шкафах) с ключевыми носителями с рабочими и/или резервными криптографическими ключами, если используется процедура опечатывания сейфов;

утрата ключей от сейфов в момент нахождения в них ключевых носителей с рабочими и/или резервными криптографическими ключами;

временный доступ посторонних лиц к ключевым носителям, а также другие события, при которых достоверно не известно, что произошло с ключевыми носителями.

6.2. В случае возникновения обстоятельств, указанных в п. 6.1 настоящей Инструкции, Пользователь обязан незамедлительно прекратить обмен электронными документами с использованием скомпрометированных закрытых криптографических ключей, по телефону информировать Администратора безопасности и Ответственного за эксплуатацию СКЗИ о факте компрометации используемых закрытых криптографических ключей.

6.3. Решение о компрометации криптографических ключей принимает руководитель Участника СЭД на основании письменного уведомления о компрометации, подписанного Ответственным за эксплуатацию СКЗИ, с приложением, при необходимости, письменного объяснения Пользователя по факту компрометации его криптографических ключей.

7. Уведомление должно содержать:

идентификационные параметры скомпрометированного криптографического ключа;

фамилию, имя, отчество Пользователя СКЗИ, который владел скомпрометированным криптографическим ключом;

сведения об обстоятельствах компрометации криптографического ключа;

время и обстоятельства выявления факта компрометации криптографического ключа.

7.1. Участник СЭД должен направить Администратору безопасности в течение одного рабочего дня с даты его информирования о факте компрометации криптографических ключей письменное «Уведомление о компрометации криптографических ключей» (далее – Уведомление о компрометации), подписанное руководителем Участника СЭД и заверенное оттиском печати Участника СЭД (Приложение 8 к Правилам ЭДО). Уведомление о компрометации должно содержать предварительно согласованные с Администратором безопасности дату и время, начиная с которых криптографические ключи считаются скомпрометированными.

7.2. Администратор безопасности после получения от Участника СЭД информации о компрометации криптографического ключа Пользователя, убеждается в достоверности полученной информации, в согласованное с Участником СЭД время выводит из действия в СЭД сертификат ключа подписи, соответствующий скомпрометированному закрытому криптографическому ключу (прекращает обмен электронными документами с использованием сертификата ключа подписи, соответствующего скомпрометированному закрытому криптографическому ключу) и проводит работу по отзыву сертификата ключа подписи Пользователя. Отозванный сертификат ключа подписи, соответствующий скомпрометированному закрытому криптографическому ключу Пользователя, помещается в список отозванных сертификатов.

7.3. Дата, начиная с которой сертификат ключа подписи считается недействительным в СЭД, устанавливается равной дате формирования списка отозванных сертификатов, в который был включен отзываемый сертификат ключа подписи.

7.4. Сертификат ключа подписи, соответствующий скомпрометированному закрытому криптографическому ключу, должен храниться Участником СЭД в течение срока хранения электронных документов для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с применением ЭЦП.

7.5. Пользователь может одновременно иметь несколько закрытых криптографических ключей и соответствующих им сертификатов ключей подписи, часть из которых использовать в качестве рабочих, а часть – в качестве резервных на случай компрометации рабочих закрытых криптографических ключей. Это обеспечивает

осуществление непрерывного электронного документооборота Участника СЭД за счет оперативного перехода на использование резервных криптографических ключей в случае компрометации рабочих криптографических ключей.

7.6. Осуществление электронного документооборота и использование СКЗИ может быть возобновлено только после ввода в действие другого криптографического ключа взамен скомпрометированного.

7.7. Скомпрометированные ключи подлежат уничтожению в соответствии с порядком, установленным в Разделе 8 настоящей Инструкции.

8. УНИЧТОЖЕНИЕ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

8.1. Неиспользованные или выведенные из действия криптографические ключи подлежат уничтожению.

8.2. Уничтожение криптографических ключей на ключевых носителях производится комиссией в составе председателя и членов комиссии, назначенной руководителем организации Участника СЭД.

8.3. Криптографические ключи, находящиеся на ключевых носителях, уничтожаются путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на СКЗИ.

8.4. При уничтожении криптографических ключей, находящихся на ключевых носителях, комиссия обязана:

установить наличие оригинала и количество копий криптографических ключей;

проверить внешним осмотром целостность каждого ключевого носителя;

установить наличие на оригинале и всех копиях ключевых носителей реквизитов путем сверки с записями в Журнале поэкземплярного учета;

убедится, что криптографические ключи, находящиеся на ключевых носителях, действительно подлежат уничтожению;

произвести уничтожение ключевой информации на оригинале и на всех копиях носителей.

8.5. О факте уничтожения криптографических ключей составляется Акт об уничтожении криптографических ключей, содержащихся на ключевых носителях (Приложение № 6 к настоящей Инструкции).

8.6. Акт об уничтожении криптографических ключей, содержащихся на ключевых носителях (далее – Акт), подписывается председателем комиссии, членами комиссии и утверждается руководителем Участника СЭД.

8.7. В Журнале поэкземплярного учета Ответственным за эксплуатацию СКЗИ производится отметка об уничтожении криптографических ключей с указанием даты и номера Акта.

8.8. Акты об уничтожении криптографических ключей, содержащихся на ключевых носителях, хранятся у Ответственного за эксплуатацию СКЗИ Участника СЭД.

9. РАЗМЕЩЕНИЕ, СПЕЦИАЛЬНОЕ ОБОРУДОВАНИЕ, ОХРАНА И ОРГАНИЗАЦИЯ РЕЖИМА В ПОМЕЩЕНИЯХ, ГДЕ УСТАНОВЛЕНЫ СКЗИ ИЛИ ХРАНЯТСЯ КРИПТОГРАФИЧЕСКИЕ КЛЮЧИ

9.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся криптографические ключи (далее – режимные помещения), должны обеспечивать сохранность СКЗИ и криптографических ключей.

9.2. При оборудовании режимных помещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

9.3. Режимные помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

9.4. Размещение, специальное оборудование, охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

9.5. Режим охраны помещений, в том числе правила допуска работников и посетителей в рабочее и нерабочее время, устанавливает Участник СЭД. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящей Инструкции.

9.6. Двери режимных помещений должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода работников и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают работникам, имеющим право допуска в режимные помещения, под расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей таких помещений следует хранить в специальном сейфе.

9.7. Для предотвращения просмотра извне режимных помещений их окна должны быть защищены.

9.8. Режимные помещения, как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным Участника СЭД. Исправность сигнализации периодически необходимо проверять с отметкой в соответствующих журналах.

9.9. Для хранения криптографических ключей, эксплуатационной и технической документации, дистрибутивов СКЗИ должно быть предусмотрено необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у Ответственного за эксплуатацию СКЗИ или работника Участника СЭД, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в специальном сейфе. Дубликат ключа от хранилища Ответственного за эксплуатацию СКЗИ в опечатанной упаковке должен быть передан на хранение должностному лицу, определенному руководителем организации Участника СЭД.

9.10. По окончании рабочего дня режимное помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны. Печати, предназначенные для опечатывания хранилищ, должны находиться у Пользователей, ответственных за эти хранилища.

9.11. В обычных условиях режимные помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только Пользователями или Ответственным за эксплуатацию СКЗИ.

9.12. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено Ответственному за эксплуатацию

СКЗИ. Ответственный за эксплуатацию СКЗИ должен оценить возможность компрометации хранящихся криптографических ключей, составить акт и принять, при необходимости, меры к локализации последствий компрометации криптографических ключей и к их замене.

9.13. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в режимных помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптографических ключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.

9.14. На время отсутствия Пользователей указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с Ответственным за эксплуатацию СКЗИ необходимо предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами в отсутствие Пользователей.

Приложение № 1
к Инструкции

ПРИКАЗ

от_____ № _____

Москва

**О назначении Ответственного
за эксплуатацию СКЗИ**

В целях организации и обеспечения эксплуатации СКЗИ в системе электронного документооборота ЗАО ВТБ Специализированный депозитарий

П Р И К А З Ы В А Ю:

1. Назначить Ответственным за эксплуатацию СКЗИ _____. Во время отсутствия _____ обязанности Ответственного за эксплуатацию СКЗИ возлагать на _____.

2. Ответственному за эксплуатацию СКЗИ при организации и обеспечении работы с СКЗИ и криптографическими ключами руководствоваться «Инструкцией по эксплуатации средств криптографической защиты информации в системе электронного документооборота Закрытого акционерного общества ЗАО ВТБ Специализированный депозитарий.

3. Контроль за исполнением настоящего приказа возложить на _____.

Руководитель _____

Приложение № 2
к Инструкции

ПРИКАЗ

от_____ № _____

Москва

О назначении Пользователя СКЗИ

В целях обеспечения и использования СКЗИ в системе электронного документооборота ЗАО ВТБ Специализированный депозитарий

П Р И К А З Ы В А Ю:

1. Назначить Пользователем СКЗИ _____.
2. Пользователю СКЗИ при работе с СКЗИ и криптографическими ключами руководствоваться «Инструкцией по эксплуатации средств криптографической защиты информации в системе электронного документооборота Закрытого акционерного общества ВТБ Специализированный депозитарий.
3. Контроль за исполнением настоящего приказа возложить на _____.

Руководитель _____

Приложение № 3
к Инструкции

Журнал
поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов

№ п.п.	Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя криптосредств	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены криптосредства	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Приложение № 4
к Инструкции

ОПИСЬ
криптографических ключей Пользователя СКЗИ

_____

(Фамилия, имя, отчество Пользователя, подразделение)

№ п/п	Дата получения	Номер криптографического ключа	Наименование СКЗИ и статус криптографического ключа	Количество ключевых носителей	Возвращено	
					Дата	Роспись
1	2	3	4	5	6	7

Приложение № 5
к Инструкции

РЕЕСТР
на передачу криптографических ключей

_____

(Фамилия, имя, отчество Пользователя, подразделение)

№ п/п	Номер криптографического ключа	Фамилия Пользователя	Количество ключевых носителей	Получено		Возвращено	
				Дата	Роспись	Дата	Роспись
1	2	3	4	5	6	7	8

Приложение № 6
к Инструкции

УТВЕРЖДАЮ

_____

_____

«____» _____ 200__ г.

АКТ № _____

об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов

г. _____ «____» _____ 200__ г.

Комиссия в составе: председателя _____; членов комиссии

_____

_____

_____ произвела уничтожение криптографических ключей, содержащихся на ключевых носителях, и ключевых документов:

№ п/п	Учетный номер ключевого носителя (документа)	Номер (идентификатор) криптографического ключа, наименование документа	Владелец ключа (документа)	Количество ключевых носителей (документов)	Номера экземпляров	Всего уничтожается ключей (документов)	Примечания
1							

Всего уничтожено XX (_____) криптографических ключей на XX (_____) ключевых носителях. Записи Акта сверены с записями в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Уничтожение криптографических ключей выполнено путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ.

Ключевые носители списаны с учета в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Председатель комиссии: _____

Члены комиссии: _____

_____