Утверждено

ЛКП.501430.58169198-07-01 34 01 ЛУ

Программная библиотека защиты информации «СКЗИ «ЛИРССЛ»

версия 1.0

Правила пользования

ЛКП.501430.58169198-07-01 34 01

Листов 23

Москва 2012 г.

СОДЕРЖАНИЕ

1. Основные технические данные и характеристики СКЗИ

Настоящие правила распространяются на программную библиотеку защиты информации «СКЗИ «ЛИРССЛ» (далее – ПБЗИ «СКЗИ «ЛИРССЛ») в вариантах исполнения 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12

ПБЗИ «СКЗИ «ЛИРССЛ» представляет средство защиты конфиденциальной информации, удовлетворяющее классу КС1 в вариантах исполнения 1-6, 11, 12; в вариантах исполнения 7-10, отличающихся использованием сертифицированного средства защиты от НСД, указанного в формуляре, и при условии обязательного опечатывания системного блока ПЭВМ - классу КС2.

ПБЗИ «СКЗИ «ЛИРССЛ» НЕ ДОПУСКАЕТСЯ защищать информацию, составляющую государственную тайну.

При встраивании СКЗИ в программные продукты и использовании автономных программных модулей СКЗИ необходимо следовать требованиям нормативных документов, входящих в состав СКЗИ.

1.1. Операционные системы

ПБЗИ «СКЗИ «ЛИРССЛ» в соответствующих вариантах исполнения предназначено для встраивания в программные продукты, работающие под управлением следующих операционных систем: Windows 2000/XP/2003/Vista (в вариантах исполнения 1, 7), Linux (в вариантах исполнения 2, 9), FreeBSD (в вариантах исполнения 3, 10), QNX (в вариантах исполнения 4, 8), Solaris 5.8 (в варианте исполнения 5), Solaris 5.9 (в варианте исполнения 6), HP-UX (в варианте исполнения 11), AIX (в варианте исполнения 12)

1.2. Реализуемые алгоритмы

Алгоритм зашифрования/расшифрования данных и вычисления имитовставки реализован в соответствии с требованиями ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая".

Алгоритм выработки значения хэш-функции реализован в соответствии с требованиями ГОСТ Р 34.11-94 "Информационная технология. Криптографическая защита информации. Функция хэширования".

Алгоритмы формирования и проверки ЭЦП реализованы в соответствии с требованиями ГОСТ Р 34.10-2001 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".

Алгоритм генерации пар открытый/закрытый ключи реализованы в соответствии с требованиями ГОСТ Р 34.10-2001 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".

1.3. Требования к ПЭВМ

СКЗИ в вариантах исполнения 1, 2, 3, 4, 7, 8, 9, 10 должно функционировать на ПЭВМ, оснащенной процессором не ниже Intel Pentium IV, НЖМД емкостью не меньше 1 Гб, ОЗУ емкостью не меньше 1 Гб, АПМДЗ (в вариантах исполнения 7, 8, 9, 10), указанном в формуляре.

СКЗИ в варианте исполнения 12 должно функционировать на автономной ПЭВМ, оснащенной процессором не ниже IBM Power Systems POWER5, НЖМД емкостью не меньше 1 Гб, ОЗУ емкостью не меньше 1 Гб.

СКЗИ в вариантах исполнения 5, 6 должно функционировать на автономной ПЭВМ, оснащенной процессором не ниже SPARCv9, НЖМД емкостью не меньше 1 Гб, ОЗУ емкостью не меньше 1 Гб.

СКЗИ в варианте исполнения 11 должно функционировать на автономной ПЭВМ, оснащенной процессором не ниже Itanium II, НЖМД емкостью не меньше 1 Гб, ОЗУ емкостью не меньше 1 Гб.

1.4. Съемные ключевые носители

К съемным ключевым носителям относятся: НГМД (3.5", 1.44 Mb); электронные USB ключи и смарт-карты eToken Pro, eToken ГОСТ; электронные USB-ключи Rutoken и Rutoken ЭЦП; универсальная электронная карта (УЭК, java-card); электронные USB ключи и смарт-карты eToken Pro (Java); устройство USB FlashDrive.

1.5. Технические характеристики ПБЗИ «СКЗИ «ЛИРССЛ»

Криптографические процедуры защиты информации ПБЗИ «СКЗИ «ЛИРССЛ» обеспечивают:

- шифрование данных по ГОСТ 28147-89 в режимах простой замены, гаммирования, гаммирования с обратной связью и в режиме сцепления блоков;
- контроль целостности данных посредством вычисления имитовставки по ГОСТ 28147-89;
- вычисление значения хэш-функции в соответствии с ГОСТ Р 34.11-94;
- вычисление и проверку электронной подписи (ЭП) в соответствии с ГОСТ Р 34.10-2001.

- ПБЗИ «СКЗИ «ЛИРССЛ» обеспечивает поддержку следующих международных криптографических стандартов: PKCS#5, PKCS#7, PKCS#8, PKCS#10, PKCS#12.

Размеры ключей имеют следующие значения:

- длина ключа для ГОСТ 28147-89 – 32 байта;
- длина ключа ЭП – 32 байта для ГОСТ Р 34.10-2001;
- длина ключа проверки ЭП – 64 байт для ГОСТ Р 34.10-2001;

Сроки действия ключей:

- максимальный срок действия закрытых ключей обмена и ЭП – 1 год 3 месяца;
- максимальный срок действия открытых ключей обмена – 1 год 3 месяца;
- максимальный срок действия сертификатов ключей проверки ЭП и ключей проверки ЭП -15 лет.

Самостоятельно ПБЗИ «СКЗИ «ЛИРССЛ» функции отображения данных, обрабатываемых с использованием средства ЭП, не реализует.

ПБЗИ «СКЗИ «ЛИРССЛ» может быть использовано в составе средств автоматического создания и (или) проверки ЭП.

При использовании ПБЗИ «СКЗИ «ЛИРССЛ» в системах без автоматического создания и (или) автоматической проверки ЭП выполнение этого требования должно возлагаться на ПО, использующее ПБЗИ «СКЗИ «ЛИРССЛ», и должно быть проверено при проведении проверок по корректности встраивания ПБЗИ «СКЗИ «ЛИРССЛ».

При встраивании ПБЗИ «СКЗИ «ЛИРССЛ» необходимо учитывать, что протокол TLS при односторонней аутентификации не обеспечивает защиты информации, хранящейся на сервере и доступной легальному клиенту. Доступ к информации, находящейся на сервере, может быть получен нарушителем в том же объеме, что и легальным пользователем.

2. Учет ключевой информации

Вся ключевая информация, находящаяся не на ключевых носителях (кроме открытых ключей), хранится в зашифрованном виде. Открытые ключи хранятся с имитозащитой, перед их использованием осуществляется проверка их целостности.

Способы формирования ключевой информации описаны в нормативных документах, входящих в состав СКЗИ.

2.1. Хранение ключевых носителей

Личные ключевые носители пользователей рекомендуется хранить в сейфе. Пользователь несет персональную ответственность за хранение личных ключевых носителей.

При наличии в организации, эксплуатирующей СКЗИ, администратора безопасности и централизованном хранении ключевых носителей, администратор безопасности организации несет персональную ответственность за хранение личных ключевых носителей пользователей. Личные ключевые носители администратора безопасности должны храниться в его личном сейфе.

2.2. Сроки действия ключей

Сроки действия ключевой информации, кроме ключей проверки ЭП не должны превышать 1 год и 3 месяца, срок действия ключей проверки ЭП – не более 15 лет.

2.3. Уничтожение ключевой информации на ключевых носителях

Ключевые носители с ключевой информацией, срок действия которой истек, не могут использоваться ни в каком другом качестве, кроме ключевого носителя ПБЗИ «СКЗИ "ЛИРССЛ". Уничтожение ключевых носителей, за исключением НГМД, осуществляется путем расплющивания молотком на наковальне. НГМД уничтожаются путем оплавления до бесформенной массы.

2.4. Компрометация ключей

Под компрометацией ключевой информации понимается разглашение информации, утрата или временная потеря ключевого носителя, копирование информации, а также несанкционированный доступ к ней.

2.5. Учет ключевой информации

В Организации, использующей ПБЗИ «СКЗИ «ЛИРССЛ» должен вестись "Журнал учета ключей", в которых следует отображать следующую информацию:

- Ф.И.О. лица, производящего запись;

- дата создания ключа;
- идентификаторы ключа (таблицы ключей) (например: серия, номер, комплект и т.п.);
- дата передачи/получения ключа;
- Ф.И.О. получателя/отправителя ключа;
- номер акта о передаче ключа или подпись получателя;
- дата установки сетевых ключей или ключей ЭП;
- дата вывода ключа из действия;
- запись о компрометации ключа;
- записи, отражающие выдачу на руки пользователям (ответственным исполнителям) и сдачу ими на хранение ключевых носителей (в случае централизованного хранения);
- администратор должен следить за сроком использования ключа ЭП.

3. Рекомендации по размещению технических средств с СКЗИ

При размещении технических средств с ПБЗИ «СКЗИ «ЛИРССЛ», следует руководствоваться следующими рекомендациями:

1. Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых установлены технические средства ПБЗИ «СКЗИ «ЛИРССЛ», посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях.
2. Рекомендуется не использовать в помещении, где размещены рабочие места с установленным ПБЗИ «СКЗИ «ЛИРССЛ», радиотелефоны и другую радиоаппаратуру.
3. Должны выполняться требования политики безопасности, принятой в организации в области размещения технических средств, обрабатывающих конфиденциальную информацию.
4. ПБЗИ «СКЗИ «ЛИРССЛ» необходимо устанавливать на ПЭВМ, разрешенные по требованиям информационной безопасности для обработки несекретной информации (конфиденциального характера), согласно принятой в информационной системе модели угроз (нарушителя).
5. В случае наличия в модели нарушителя угроз по защите от ПЭМИН, защита СКЗИ может быть обеспечена при установке СКЗИ на ПЭВМ, удовлетворяющие требованиям информационной безопасности, например СТР-К. При этом защита должна быть обеспечена использованием соответствующих оптических развязывающих устройств, устанавливаемых в тракте передачи информации (при его наличии) - линии связи, выходящей за пределы контролируемой зоны.
6. В случае отсутствия в модели нарушителя угроз по защите от ПЭМИН данное требование носит рекомендательный характер.
7. При размещении ПЭВМ с СКЗИ в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну или конфиденциального характера, данные ПЭВМ должны иметь соответствующее разрешение.

4. Требования к программному и аппаратному обеспечению

1. На технических средствах, оснащенных ПБЗИ «СКЗИ «ЛИРССЛ», должно использоваться только лицензионное программное обеспечение фирм-производителей. Указанное ПО не должно содержать средств разработки и отладки приложений, а также содержать в себе возможностей, позволяющих оказывать воздействие на функционирование ПБЗИ «СКЗИ «ЛИРССЛ». В случае технологических потребностей организации, эксплуатирующей СКЗИ, в использовании иного программного обеспечения, его применение должно быть санкционировано администратором безопасности. В любом случае ПО не должно содержать в себе возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;
- модифицировать собственный код и код других подпрограмм;
- модифицировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;
- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- использовать недокументированные фирмами-разработчиками функции.

2. На ПЭВМ одновременно может быть установлена только одна ОС из поддерживаемых (п. 1.1).

3. В BIOS ПЭВМ определяются установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске: отключается возможность загрузки с гибкого диска, привода CD-ROM и прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Не применяются ПЭВМ с BIOS, исключающим возможность отключения сетевой загрузки ОС.

4. Средствами BIOS должна быть исключена возможность отключения пользователями PCI устройств при использовании ПАК защиты от НСД, устанавливаемых в PCI разъем.

5. Вход в BIOS ПЭВМ должен быть защищен паролем. Пароль для входа в BIOS должен быть известен только администратору и быть отличным от пароля администратора для входа в ОС.

6. Средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты.

7. Программные модули, использующие ПБЗИ «СКЗИ «ЛИРССЛ» (прикладного ПО со встроенной ПБЗИ «СКЗИ «ЛИРССЛ»), должны быть доступны только по чтению/запуску (в атрибутах файлов запрещена запись и модификация).

8. Администратором безопасности должно быть проведено опечатывание системного блока с установленным ПБЗИ «СКЗИ «ЛИРССЛ», исключающее возможность несанкционированного изменения аппаратной части рабочей станции.

9. При эксплуатации ПАК «Аккорд-АМДЗ» в составе ПБЗИ «СКЗИ «ЛИРССЛ», должны выполняться требования, изложенные в нормативных документах, входящих в состав ПАК «Аккорд-АМДЗ».

5. Требования к продолжительности функционирования ПЭВМ

Не допускается непрерывное функционирование ПЭВМ с установленным СКЗИ более суток (24 часов) без аппаратной перезагрузки ПЭВМ.

6. Требования по защите от НСД

ПБЗИ «СКЗИ «ЛИРССЛ» при условии выполнения настоящих Правил обеспечивает защиту конфиденциальной информации по уровню КС1 для вариантов исполнения №1-№6 и №11-№12, а также по уровню КС2 - для вариантов исполнения №7-№10.

6.1. 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 ПЭВМ и ее средств;
- администрирование информационной безопасности;
- учет носителей информации;
- сигнализация о попытках нарушения защиты;
- периодическое тестирование технических и программных средств защиты;
- использование сертифицированных и лицензионных программных и технических 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 быть либо периодическим, либо инициироваться по мере необходимости пользователем или контролирующими органами.

В организации - пользователе системы должно быть выделено специальное должностное лицо - администратор безопасности, функции которого должны заключаться в выполнении процедур установки ПО, настройки системного окружения, установки, настройки, обслуживания и обеспечения функционирования средств защиты.

Администратор безопасности должен иметь возможность доступа ко всей информации, обрабатываемой на рабочем месте.

Каждый исполнитель работ как пользователь сети конфиденциальной связи должен быть зарегистрирован у администратора службы безопасности.

В организации - пользователе системы должны вестись "Журналы регистрации администраторов и пользователей" (возможно ведение одного журнала для всей организации), в которые заносятся следующие данные:

- Ф.И.О. регистрируемого лица;

- название подразделения организации (при ведении общего журнала);
- степень его допуска (администратор/пользователь);
- дата регистрации;
- дата окончания срока действия регистрации.

6.2. Организационные меры защиты информации от НСД

При использовании ПБЗИ «СКЗИ «ЛИРССЛ» следует принять следующие организационные меры:

1. Право доступа к рабочим местам с установленным ПО ПБЗИ «СКЗИ «ЛИРССЛ» должно предоставляться только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на программное обеспечение, имеющее в своем составе ПБЗИ «СКЗИ «ЛИРССЛ».
2. Запретить осуществление несанкционированного администратором безопасности копирования ключевых носителей.
3. Запретить передачу ключевых носителей и других ключевых документов лицам, к ним не допущенным.
4. Запретить использование ключевых носителей в режимах, не предусмотренных правилами пользования ПБЗИ «СКЗИ «ЛИРССЛ», либо использовать ключевые носители на посторонних ПЭВМ.
5. Запретить запись на ключевые носители посторонней информации.
6. Запретить оставлять без контроля вычислительные средства, на которых эксплуатируется ПБЗИ «СКЗИ «ЛИРССЛ» после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки.

6.3. Организационно-технические меры защиты от НСД

Должен быть реализован следующий комплекс организационно-технических мер защиты от НСД:

1. Перед началом процесса установки ПО со встроенными модулями СКЗИ либо автономных программных модулей СКЗИ должен осуществляться контроль целостности устанавливаемого ПО утилитой check_distr_hash, входящей в состав СКЗИ (см. Руководство администратора).
2. При каждом запуске ПЭВМ с установленным ПБЗИ «СКЗИ «ЛИРССЛ» должен осуществляться контроль целостности программного обеспечения, входящего в состав

ПБЗИ «СКЗИ «ЛИРССЛ», самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ.

3. В случае обнаружения "посторонних" (не зарегистрированных) программ или нарушения целостности программного обеспечения работа должна быть прекращена.

4. При использовании ПБЗИ «СКЗИ «ЛИРССЛ» в вариантах исполнения №1-№6 и №11-№12:

- Контроль целостности должен осуществляться утилитой check_hash и сторонними сертифицированными средствами, входящей в состав ПБЗИ «СКЗИ «ЛИРССЛ»
- Администратор должен периодически (не реже 1 раза в год) менять пароль на вход в BIOS.
- Средствами BIOS ПЭВМ для пользователя должен быть установлен пароль входа в систему.
- Длина пароля не должна быть менее 6 символов.

5. При использовании ПБЗИ «СКЗИ «ЛИРССЛ» в вариантах исполнения №7-№10:

- Контроль целостности программной среды должен осуществляться средствами ПАК "Аккорд-АМДЗ".
- Должна быть подключена блокировка ПЭВМ через специальный кабель питания АТХ, входящий в состав ПАК "Аккорд-АМДЗ", который подключается вместе со штатным кабелем питания АТХ к блоку питания и системной плате ПЭВМ.
- Должна быть исключена возможность работы пользователей на ПЭВМ с установленным ПАК "Аккорд-АМДЗ" до регистрации администратора и настройки им параметров работы АПМДЗ.
- После установки и настройки ПАК "Аккорд-АМДЗ" в обязательном порядке должна быть исключена возможность бесконтрольного доступа к техническим средствам АПМДЗ и ПЭВМ, установленных внутри корпуса системного блока ПЭВМ, со стороны любых субъектов за исключением администратора АПМДЗ, в функциональные обязанности которого входит обеспечение правильности функционирования АПМДЗ.
- ПАК "Аккорд-АМДЗ" обеспечивает блокировку загрузки ОС с CD-ROM, Floppy дисководов. АПМДЗ обеспечивает блокировку загрузки ОС с устройств с интерфейсами USB и IEEE 1994 при условии поддержки системным BIOS ПЭВМ 48h функции 13 прерывания. Если системный BIOS ПЭВМ не поддерживает 48h функцию 13 прерывания, то блокировка

загрузки ОС с устройств с интерфейсами USB и IEEE 1994 должна быть осуществлена организационно техническими мерами. Блокировка загрузки ОС с других типов внешних носителей должна быть осуществлена организационно-техническими мерами.

- При эксплуатации ПАК "Аккорд-АМДЗ" на ПЭВМ, на котором обрабатывается конфиденциальная информация и не проведена проверка BIOS на отсутствие аппаратно-программных механизмов, ориентированных на целенаправленное нарушение правильности функционирования АПМДЗ, необходимо организационно техническими мероприятиями осуществить блокировку загрузки ОС с устройств с интерфейсами USB и IEEE 1394.
- При конфигурировании ПАК "Аккорд-АМДЗ" администратором должны быть установлены следующие сроки действия: персонального идентификатора – не более 365 дней.
- Техническое обслуживание ПАК "Аккорд-АМДЗ" (регламентные работы) должно проводиться не реже одного раза в год.
- Для своевременного выявления нарушений в работе ПАК "Аккорд-АМДЗ" с помощью встроенных процедур тестирования компонентов изделия необходимо осуществлять перезагрузку ПЭВМ не реже одного раза в сутки.
- Не допускается использование функции Quick Boot в случае применения на защищаемой ПЭВМ менеджера оперативной памяти QEMM, а также аналогичных функций, реализованных в других программных пакетах.
- Не допускается использование на защищаемой ПЭВМ менеджера загрузки операционных систем Advance Boot Manager, а также других программных продуктов, реализующих аналогичные функции.

6. Пользователь должен запускать только те приложения, которые разрешены администратором.

7. Администратор безопасности должен сконфигурировать операционную систему, в среде которой планируется использовать ПБЗИ «СКЗИ «ЛИРССЛ», и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

- Не использовать нестандартные, измененные или отладочные версии ОС.
- Исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой.

- Исключить возможность удаленного управления, администрирования и модификации ОС и её настроек.
- На ПЭВМ должна быть установлена только одна операционная система.
- Правом установки и настройки ОС и ПБЗИ «СКЗИ «ЛИРССЛ» должен обладать только администратор безопасности.
- ОС должна быть настроена только для работы с ПБЗИ «СКЗИ «ЛИРССЛ». Все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.).
- Режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень.
- Всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права.
- Необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):
    - системный реестр;
    - файлы и каталоги;
    - временные файлы;
    - журналы системы;
    - файлы подкачки;
    - кэшируемая информация (пароли и т.п.);
    - отладочная информация.

Кроме того, необходимо организовать затирание (по окончании сеанса работы СКЗИ) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ. Если это не выполнимо, то ОС должна использоваться в однопользовательском режиме и на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.

Примечание: *Под однопользовательским режимом в данном случае подразумевается такой режим, при котором все пользователи данной рабочей станции имеют одинаковый комплект ключевой информации этой рабочей станции. Одновременная работа нескольких пользователей на одной ПЭВМ, в том числе с использованием протоколов удаленного взаимодействия должна быть исключена.*

- Должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии.

- Необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а так же исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС.
- В случае подключения ПЭВМ с установленной ПБЗИ «СКЗИ «ЛИРССЛ» к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (JavaScript, VBScript, ActiveX), полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.
- При использовании ПБЗИ «СКЗИ «ЛИРССЛ» на ПЭВМ, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют ПБЗИ «СКЗИ «ЛИРССЛ», и к компонентам ПБЗИ «СКЗИ «ЛИРССЛ» со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN сетей и т.п.). При этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации.
- Организовать и использовать систему аудита, организовать регулярный анализ результатов аудита.
- Организовать и использовать комплекс мероприятий антивирусной защиты.
- Исключить одновременную работу в ОС с работающим ПБЗИ «СКЗИ «ЛИРССЛ» и загруженной ключевой информацией нескольких пользователей.

6.4. Программно-технические средства защиты от НСД

Программно-аппаратный комплекс (ПАК) "Аккорд-АМДЗ" предназначен для защиты информации от НСД при ее обработке в ПЭВМ.

ПАК "Аккорд-АМДЗ" обеспечивает:

1. идентификацию, проверку подлинности, разграничение доступа к ресурсам ПЭВМ на уровне выполняемых задач и контроль доступа субъектов в систему (ПЭВМ);
2. регистрацию и учет входа (выхода) пользователей в систему (из системы), доступа пользователей к защищаемым файлам, изменения полномочий пользователей;
3. обеспечение целостности программных средств.

Установка и настройка ПАК "Аккорд-АМДЗ" на АРМ пользователя должна производиться в соответствии с эксплуатационной документацией на ПАК "Аккорд-АМДЗ". Перед эксплуатацией ПАК "Аккорд-АМДЗ" в составе АРМ пользователя необходимо ознакомиться с комплектом документации на данный комплекс и принять рекомендуемые в документации защитные организационные меры.

Установка программного обеспечения и аппаратной части комплекса "Аккорд-АМДЗ" на АРМ может выполняться специалистами поставщика ПБЗИ «СКЗИ «ЛИРССЛ» или представителями службы информационной безопасности. Настройка комплекса "Аккорд-АМДЗ" на требуемую конфигурацию выполняется администратором безопасности. Настройка должна исключать возможность вмешательства пользователя в процессы загрузки операционной системы и прикладного ПО и проверки целостности программной среды.

7. Требования по встраиванию ПБЗИ «СКЗИ «ЛИРССЛ».

При встраивании необходимо соблюдать следующие требования:

- Проводить инициализацию ДСЧ в соответствии с пунктом 4.2 ПБЗИ «СКЗИ «ЛИРССЛ» Руководство администратора ЛКП 501430.58169198-07-01 34 02. По завершению инициализации должна быть проверена корректность работы библиотечных функций RAND_seed(), RAND_add().
- Должна быть обеспечена возможность доступа к файлам и ветвям реестра, в которых хранятся инициализационные векторы ДСЧ только пользователям СКЗИ. Инициализацию и переинициализацию ДСЧ может производить только администратор СКЗИ и только описанным в пункте 4.2 ПБЗИ «СКЗИ «ЛИРССЛ» Руководство администратора ЛКП 501430.58169198-07-01 34 02 способом. Изменять и произвольным образом задавать данные инициализационного вектора запрещено.
- Должна быть обеспечена конфиденциальность ключевых носителей. Запрещается передавать третьим лицам, копировать и бесконтрольно распространять ключевую информацию, используемую в ПБЗИ «СКЗИ «ЛИРССЛ».
- Должна быть обеспечена невозможность модификации нарушителем конфигурационного файла ПБЗИ «СКЗИ «ЛИРССЛ» - lirssl.cnf.

При встраивании по исходным текстам ПО, использующего функции ПБЗИ «СКЗИ «ЛИРССЛ», необходимо проверить:

- Корректность инициализации (деинициализации) ПБЗИ «СКЗИ «ЛИРССЛ» (обработка кода возврата функции инициализации).
- Корректность вызова ПБЗИ «СКЗИ «ЛИРССЛ» (передаваемые параметры должны быть должным образом инициализированы, последовательность вызовов должна соответствовать описанию, приведенному в ПБЗИ «СКЗИ «ЛИРССЛ» Руководство разработчика ЛКП 501430.58169198-07-01 33 01).
- Корректность обработки ошибочных ситуаций.
- При использовании функций протоколов TLS и SSL, использующих сервисы инфраструктуры открытых ключей, должен использоваться сертифицированный по соответствующему классу на соответствие требованиям ФСБ удостоверяющий центр.

При использовании ПБЗИ «СКЗИ «ЛИРССЛ» в системах без автоматического создания и (или) автоматической проверки ЭП ПО, использующее ПБЗИ «СКЗИ «ЛИРССЛ» должно реализовывать следующие функции:

при создании ЭП:

- показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;
- создавать ЭП только после подтверждения лицом, подписывающим электронный документ, операции по созданию ЭП;
- однозначно показывать, что ЭП создана.

При проверке ЭП средства ЭП должны:

- показывать содержание электронного документа, подписанного ЭП;
- показывать информацию о внесении изменений в подписанный ЭП электронный документ;
- указывать на лицо, с использованием ключа ЭП которого подписаны электронные документы.

8. Требования по проведению периодического контроля

1. ПБЗИ «СКЗИ «ЛИРССЛ» и технические средства, на которых он эксплуатируется должны подвергаться периодическому контролю и тестированию.
2. Периодическое тестирование должно проводиться в соответствии с требованиями, существующими в организации, но не реже одного раза в 10 дней.
3. Процесс тестирования заключается в:
    - перезапуске рабочей станции
    - проведении тестирования аппаратного модуля доверенной загрузки в соответствии с требованиями документации разработчиков модуля (только для вариантов исполнения №7-№10)
    - проверки правильности конфигурации и установленных прав доступа к файлам ПБЗИ «СКЗИ «ЛИРССЛ» (см. Руководство Администратора)
    - контроле целостности файлов ПБЗИ «СКЗИ «ЛИРССЛ» (осуществляется либо с помощью самой ПБЗИ «СКЗИ «ЛИРССЛ», либо сторонними сертифицированными средствами).
4. При возникновении ошибок в процессе тестирования необходимо остановить работу комплекса и известить администратора и разработчиков ПБЗИ «СКЗИ «ЛИРССЛ».

9. Перечень программных модулей СКЗИ, целостность которых необходимо контролировать

Перечень программных модулей СКЗИ, входящих в состав дистрибутивов для операционных систем семейства MS Windows:

- liblircrypto.dll (Библиотека криптографических преобразований)
- liblirssl.dll (Библиотека поддержки протоколов SSL/TLS)
- lirssl.exe (Утилита командной строки)
- lirssl_conf.cnf (Файл конфигурации утилиты командной строки)
- check_hash.exe (Модуль контроля целостности)
- msvcr71.dll (Библиотека Windows, необходимая для работы СКЗИ)
- zamok.dll (Библиотека для взаимодействия с АПМДЗ)

Перечень программных модулей СКЗИ, входящих в состав дистрибутивов для операционных систем семейства UNIX:

- liblircrypto.so.0.9.7 (Библиотека криптографических преобразований)
- liblirssl.so.0.9.7 (Библиотека поддержки протоколов SSL/TLS)
- lirssl (Утилита командной строки)
- lirssl.cnf (Файл конфигурации)
- lirssl_conf.cnf (Файл конфигурации утилиты командной строки)
- check_hash (Модуль контроля целостности)
- zamok.so (Библиотека для взаимодействия с АПМДЗ)
- LirSSL_uninstall.pl (Деинсталляционный скрипт)

10.ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Основание (вх. № сопроводительного документа и дата)	Дата проведения изменения	Содержание изменения	Должность, фамилия и подпись лица, ответственного за изменения	Подпись лица, ответственного за эксплуатацию изделия