# Выдержки из согласованных с ФСБ России «Правил пользования…» поставляемыми для работы в системе «iBank 2» криптобиблиотеками

**Оглавление**

# 1. Введение

В данном документе содержатся выдержки из согласованных с ФСБ России «Правил пользования…» поставляемыми для работы в системе «iBank 2» криптобиблиотеками:

- программная библиотека защиты информации (ПБЗИ) «Крипто-Си» Версия 2.0, все исключительные права на которую принадлежат ООО «КриптоЭкс»;
- средство криптографической защиты информации (СКЗИ) «Крипто-КОМ 3.3», все исключительные права на которую принадлежат ЗАО «Сигнал-КОМ».
- СКЗИ «ФОРОС. Исполнение №1», разработки ООО «СмартПарк».

В данных выдержках определены организационно-технические и административные мероприятия при использовании СКЗИ (ПБЗИ), обязательные для исполнения пользователями СКЗИ (ПБЗИ).

# 2. Организационно-технические и административные мероприятия при использовании программных СКЗИ

## 2.1. Общие положения

Защита аппаратного и программного обеспечения от НСД при установке и использовании программных криптобиблиотек СКЗИ «Крипто-КОМ 3.3» , ПБЗИ «Крипто-Си» Версия 2.0 является составной частью общей задачи обеспечения безопасности информации в системе, в состав которой входит СКЗИ.

Наряду с применением средств защиты от НСД необходимо выполнение целого ряда мер, включающего в себя организационно-технические и административные мероприятия, связанные с обеспечением правильности функционирования технических средств обработки и передачи информации, а также установление соответствующих правил для обслуживающего персонала, допущенного к работе с конфиденциальной информацией.

В приведенных ниже разделах, содержатся основные требования по выполнению указанных мер защиты.

## 2.2. Организация работ по защите от НСД

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 должен периодически выполняться администратором безопасности на основе требований документации на средства защиты от НСД.

В организации, эксплуатирующей СКЗИ (ПБЗИ), должен быть назначен администратор безопасности, на которого возлагаются задачи организации работ по использованию СКЗИ (ПБЗИ), выработки соответствующих инструкций для пользователей, а также контроль над соблюдением описанных ниже требований.

Правом доступа к рабочим местам с установленными СКЗИ (ПБЗИ) должны обладать только определенные для эксплуатации лица, прошедшие соответствующую подготовку. Администратор безопасности должен ознакомить каждого пользователя, применяющего СКЗИ (ПБЗИ), с документацией на СКЗИ (ПБЗИ), а также с другими нормативными документами, созданными на её основе.

## 2.3 Требования по размещению технических средств с установленным СКЗИ (ПБЗИ)

При размещении технических средств с установленным СКЗИ (ПБЗИ):

- Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным СКЗИ, посторонних лиц, по роду своей деятельности, не являющихся персоналом, допущенным к работе в этих помещениях.
- Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ, сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию

- Размещение СКЗИ в помещениях, в которых осуществляется обработка информации, содержащей сведения, составляющие государственную тайну, осуществляется установленным порядком.

# 3. СКЗИ «Крипто-КОМ 3.3»

## 3.1 Требования по установке СКЗИ, а также общесистемного и специального ПО на ПЭВМ

К установке общесистемного и специального программного обеспечения, а также СКЗИ, допускаются лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее ПО и на СКЗИ.

При установке программного обеспечения СКЗИ следует:

- На технических средствах, предназначенных для работы с СКЗИ использовать только лицензионное программное обеспечение фирм-изготовителей.
- В случае если в модели угроз, которым должно противостоять СКЗИ в информационной системе заказчика, признана опасной утечка по техническим каналам, ЭВМ, на которых устанавливается СКЗИ, должны быть допущены для обработки информации по действующим в Российской Федерации требованиям по защите информации от утечки по техническим каналам, в том числе, по каналу связи (например, СТР-К).
- Инсталляция СКЗИ на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу.
- При установке ПО СКЗИ на ЭВМ должен быть обеспечен контроль целостности и достоверность дистрибутива СКЗИ и совместно поставляемых с СКЗИ компонент среды функционирования (СФ).
- На ЭВМ не должны устанавливаться средства разработки ПО и отладчики. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором безопасности. При этом должны быть реализованы меры, исключающие возможность использования этих средств для редактирования кода и памяти СКЗИ и приложений, использующих СКЗИ, а также для просмотра кода и памяти СКЗИ и приложений, использующих СКЗИ, в процессе обработки СКЗИ защищаемой информации и/или при загруженной ключевой информации.
- Предусмотреть меры, исключающие возможность несанкционированного не обнаруживаемого изменения аппаратной части технических средств, на которых установлены СКЗИ (например, путем опечатывания системного блока и разъемов ЭВМ).
- После завершения процесса установки должны быть выполнены действия, необходимые для осуществления периодического контроля целостности установленного ПО СКЗИ, а также его окружения в соответствии с документацией.
- Программное обеспечение, устанавливаемое на ЭВМ с СКЗИ, не должно содержать 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;
- повышать предоставленные привилегии;
- модифицировать настройки ОС;
- использовать недокументированные фирмой-разработчиком функции ОС.

### 3.2 Требования по защите от НСД при эксплуатации СКЗИ

При организации работ по защите информации от НСД необходимо учитывать следующие требования:

- Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:
  - длина пароля должна быть не менее 6 символов при мощности алфавита не менее 10;
  - в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
  - пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (USER, ADMIN и т.д.);
  - при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
  - личный пароль пользователь не имеет права сообщать никому;
  - периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6 месяцев.

  Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС.
- Средствами BIOS должна быть исключена возможность работы на ЭВМ с СКЗИ, если во время её начальной загрузки не проходят встроенные тесты.
- Запрещается:
  - оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации либо иной конфиденциальной информации;
  - вносить какие-либо изменения в программное обеспечение СКЗИ;
  - осуществлять несанкционированное администратором безопасности копирование ключевых носителей;

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;
- записывать на ключевые носители постороннюю информацию;
- работать с СКЗИ при неисправности средств защиты от НСД.

Администратор безопасности должен сконфигурировать операционную систему, в среде которой планируется использовать СКЗИ, 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 ЭВМ должна быть установлена только одна операционная система.
- Правом установки и настройки ОС и СКЗИ должен обладать только администратор безопасности.
- 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 невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.

- 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 также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС.
- В случае подключения ЭВМ с установленным СКЗИ к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (например, 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 СКЗИ на ЭВМ, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN 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.
- СКЗИ должно использоваться со средствами антивирусной защиты, сертифицированными ФСБ России. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.
- Должно быть запрещено использование СКЗИ для защиты речевой информации без проведения соответствующих дополнительных исследований.
- При работе СКЗИ должны быть отключены средства выхода в радиоканал.
- Необходимо проводить перезагрузку ЭВМ с СКЗИ не реже одного раза в неделю.

СКЗИ «Крипто-КОМ 3.3» в исполнении 1 (уровень КС1) при условии выполнения настоящих рекомендаций обеспечивают защиту конфиденциальной информации от внешнего нарушителя, самостоятельно осуществляющего создание методов и средств реализации атак, а также самостоятельно реализующего атаки.

СКЗИ «Крипто-КОМ 3.3» в исполнении 2 (уровень КС2) при условии выполнения настоящих рекомендаций и использовании дополнительных средств защиты от НСД обеспечивают защиту конфиденциальной информации также от внутреннего нарушителя, не являющегося пользователем средств вычислительной техники, на которых реализованы СКЗИ, самостоятельно осуществляющего создание методов и средств реализации атак, а также самостоятельно реализующего атаки. Механизмы аутентификации, используемые средствами защиты от НСД, должны ограничивать количество следующих подряд попыток аутентификации субъекта доступа, число которых не должно быть больше 10. При превышении установленного предельного числа следующих подряд попыток аутентификации доступ должен блокироваться на промежуток времени, определяемый условиями эксплуатации СКЗИ в конкретной автоматизированной системе.

СКЗИ «Крипто-КОМ 3.3» в исполнении 2 обеспечивает уровень защищенности класса КС2 при совместном использовании с любым программно-аппаратным комплексом (ПАК) защиты от НСД, сертифицированным ФСБ России по требованиям, выдвигаемым к электронным замкам.

При отсутствии реализации ПАК защиты от НСД для требуемой платформы СКЗИ «Крипто-КОМ 3.3» обеспечивает уровень защищенности класса КС2 только при выполнении следующих требований по защите от НСД:

- процессорный блок и устройства загрузки ЭВМ должны быть опечатаны;
- конфиденциальная информация не должна храниться в открытом виде;
- на ЭВМ не должны использоваться средства разработки и отладки.
- СКЗИ должно использоваться со средствами защиты от компьютерных вирусов и компьютерных атак, сертифицированными ФСБ России; класс средств защиты от компьютерных вирусов и компьютерных атак определяется условиями эксплуатации СКЗИ в автоматизированных системах.

## 3.3 Обеспечение безопасности функционирования рабочих мест со встроенным СКЗИ

В данном разделе представлены основные рекомендации по организационно-техническим мерам защиты для обеспечения безопасности функционирования рабочих мест со встроенным СКЗИ.

- Использование шифровальных средств для криптографической защиты информации подлежит лицензированию в соответствии с действующим законодательством РФ.
- Рабочие места, на которые установлены СКЗИ, должны быть аттестованы комиссией. Результаты работы комиссии отражаются в «Акте готовности к работе» (см. Приложение).
- Должностные инструкции администратора безопасности (его заместителя) и ответственного исполнителя должны учитывать требования настоящих рекомендаций.
- При каждом включении рабочей станции с установленным СКЗИ необходимо проверять сохранность печатей системного блока и разъемов рабочей станции.
- Санкционированное снятие и установка приспособлений для опечатки системного блока и разъемов рабочей станции с установленным СКЗИ должно фиксироваться в соответствующем журнале.
- ЭВМ должна обладать средствами самотестирования при включении питания, а также средствами контроля уровня питающих напряжений и прерывания работы компьютера при снижении напряжений ниже допустимых пределов. При эксплуатации ЭВМ с установленным СКЗИ допускается одно промежуточное выключение питания в течение суток при круглосуточном режиме работы.
- При необходимости удаления файлов, которые использовались при работе СКЗИ, реализовать физическое затирание содержимого удаляемых файлов с помощью утилиты wipe из состава СКЗИ.
- В случае обнаружения «посторонних» (незарегистрированных) программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на АРМ должна быть прекращена. По данному факту

должно быть проведено служебное расследование комиссией в составе представителей служб информационной безопасности организации - владельца сети и организации - абонента сети, где произошло нарушение, и организованы работы по анализу и ликвидации негативных последствий данного нарушения.

- Пользователь должен запускать только те приложения, которые разрешены администратором безопасности
- Криптографические приложения, созданные на базе СКЗИ «Крипто-КОМ 3.3» должны быть выполнены в соответствии с «Инструкцией по встраиванию».

Не допускается:

- Использовать режим простой замены ГОСТ 28147-89 для шифрования информации, кроме ключевой.
- Подключать к ЭВМ дополнительные устройства и соединители, не предусмотренные штатной комплектацией.
- Обрабатывать на ЭВМ, оснащенной СКЗИ, информацию, содержащую государственную тайну.
- Использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ.
- Осуществлять несанкционированное вскрытие системных блоков ЭВМ.
- Приносить и использовать в помещении, где установлены средства СКЗИ, радиотелефоны и другую радиопередающую аппаратуру (требование носит рекомендательный характер).

# Приложение. Акт готовности к работе

**УТВЕРЖДАЮ**

_____

(должность)

_____

(наименование учреждения)

_____

(подпись) (Ф.И.О.)

АКТ

готовности к работе _____ с _____

(наименование учреждения) (наименование изделий)

«_____» _____ 20___г.

Комиссия в составе председателя _____

(должность) (Ф.И.О.)

и

членов_____

_____

назначенная _____ составила настоящий акт о том, что помещение

эксплуатирующего органа_____, размещение _____,

(название) (оборудование)

хранилища ключевых документов, охрана помещений и подготовленность сотрудников к обслуживанию

_____

(оборудование)

соответствуют:_____

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

Комиссия отмечает, что инсталляция ПО вышеупомянутых изделий проведена в соответствии с

_____

(инструкции)

Вывод: комиссия считает, что объект_____ отвечает требованиям (название объекта)

_____

(название инструкции)

по обеспечению безопасности связи по уровню _____ и может быть введен в действие.

Председатель:

_____ _____

(подпись) (Ф.И.О)

Члены комиссии

_____ _____

(подпись) (Ф.И.О)

_____ _____

(подпись) (Ф.И.О)

_____ _____

(подпись) (Ф.И.О)

М.П.

# 4. ПБЗИ «Крипто-Си» Версия 2.0

## 4.1 Требования по установке ПБЗИ, а также общесистемного и специального ПО на ПЭВМ

К установке общесистемного и специального программного обеспечения, а также ПБЗИ, допускаются лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее ПО и на ПБЗИ.

При установке программного обеспечения ПБЗИ следует:

- На технических средствах, предназначенных для работы с ПБЗИ, использовать только лицензионное программное обеспечение фирм - изготовителей.
- Установку ПБЗИ на ЭВМ должна производиться только с зарегистрированного, защищенного от записи лицензионного носителя.
- На ЭВМ исключить установку средств разработки ПО и отладчики. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором безопасности. При этом должны быть реализованы меры, исключающие возможность использования этих средств для редактирования кода и памяти ПБЗИ и приложений, использующих ПБЗИ, а также для просмотра кода и памяти ПБЗИ и приложений, использующих ПБЗИ, в процессе обработки ПБЗИ защищаемой информации и/или при загруженной ключевой информации.
- Предусмотреть меры, исключающие возможность несанкционированного не обнаруживаемого изменения аппаратной части технических средств, на которых установлены ПБЗИ (например, путем опечатывания системного блока и разъемов ЭВМ).
- После завершения процесса установки выполнить действия, необходимые для осуществления периодического контроля целостности установленного ПБЗИ, а также его окружения в соответствии с документацией.
- Из программного обеспечения, устанавливаемого на ЭВМ с ПБЗИ исключить содержащее возможности, позволяющие:
  - 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;
  - повышать предоставленные привилегии;
  - модифицировать настройки ОС;
  - использовать недокументированные фирмой-разработчиком функции ОС.

Эксплуатация программных и аппаратно-программных комплексов со встроенной в них ПБЗИ «Крипто-Си» Версия 2. должна проводиться на персональных компьютерах с организованным контролем целостности программной среды. Для выполнения периодических

проверок необходимо использовать разработанные средства контроля целостности модулей ПБЗИ и операционной системы.

Необходимо обеспечить контроль целостности отдельных компонентов операционных систем и модулей ПБЗИ.

Проверка целостности модулей ПБЗИ может быть осуществлена с использованием:

- filehash, файла подписи ПБЗИ и файл с открытым ключом;
- check_bibl и таблицы проверочных значений.

Приведённые программные средства, файл подписи (содержит хэш – значение и подпись, выработанную на закрытом ключе разработчика ПБЗИ) и файл с открытым ключом поставляются с ПБЗИ. Таблица проверочных значений поставляется в виде печатного документа, а так же может создаваться проверяющим (сертифицирующем) органом.

При проведении тематических исследований для всех исполняемых модулей ПБЗИ вычисляется значение хэш-функции и формируется ЭЦП на закрытом ключе разработчика. Для проверки целостности модулей с использованием filehash необходимо в каталоге расположения файлов ПБЗИ запустить программу, подав ей на вход файл подписи и файл открытого ключа разработчика. Filehash проверит подписи для каждого файла, входящего в поставляемую ПБЗИ, используя для этого открытый ключ разработчика. Для каждого файла в случае успешной проверки будет выведено сообщение “имя файла ПБЗИ OK+! ”.

Средство check_bibl, обеспечивает возможность проверки целостности модуля библиотеки с использованием таблицы контрольных значений. Каждая запись таблицы включает две сущности: ключ, проверочное значение. При проверке пользователь вводит выбранный ключ из выше указанной таблицы, на основании введённого ключа осуществляется вычисление проверочного значения, отображаемое на консоли пользователя. Установление целостности осуществляется пользователем путем визуального сравнения полученного значения с табличным значением, соответствующим введённому ключу.

Проверка целостности компонентов операционной системы может осуществляется с помощью поставляемых вместе с ПБЗИ программ filehash и filechck:

Программа filehash предназначена для вычисления значения хэш-функции, если задано только имя файла, и цифровой подписи файла, если задан еще ключевой контейнер с закрытым ключом. В первом режиме работы в результате выдается имя файла, значение хэш-функции, во втором – еще и подпись.

Программа filechck осуществляет проверку подписи для указанного файла. Для ее работы необходимо задать имя файла, открытый ключ и подпись.

Контроль целостности компонентов операционной системы рекомендуется проводить не реже одного раза в полгода. В случае обнаружения изменений в перечисленных компонентах системы не рекомендуется продолжать эксплуатацию ПБЗИ. В случае внесения изменений в указанные компоненты операционной системы следует внести соответствующие изменения в параметры процедуры проверки целостности.

### 4.2 Требования по защите от НСД при эксплуатации ПБЗИ

При организации работ по защите информации от НСД необходимо обеспечить выполнение следующих требований:

- Право доступа к рабочим местам с установленным ПБЗИ должно предоставляется только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на ПБЗИ.
- Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:
  - длина пароля должна быть не менее 6 символов;
  - в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п .);
  - пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);
  - при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
  - личный пароль пользователь не имеет права сообщать никому;
  - периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6 месяцев.

  Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС.
- Средствами BIOS должна быть исключена возможность работы на ЭВМ с ПБЗИ, если во время её начальной загрузки не проходят встроенные тесты.
- Вход в BIOS ЭВМ должен быть защищен паролем, к которому предъявляются те же требования, что и к паролю администратора системы. Пароль для входа в BIOS должен быть известен только администратору системы и быть отличным от пароля администратора для входа в систему.

Запрещается:

- оставлять без контроля вычислительные средства, на которых эксплуатируется ПБЗИ, после ввода ключевой информации либо иной конфиденциальной информации;
- вносить какие-либо изменения в программное обеспечение ПБЗИ;
- осуществлять несанкционированное администратором безопасности копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных функционированием ПБЗИ;
- записывать на ключевые носители постороннюю информацию.

Администратор безопасности должен сконфигурировать операционную систему, в среде которой планируется использовать ПБЗИ, 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 ЭВМ должна быть установлена только одна операционная система;
- правом установки и настройки ОС и ПБЗИ должен обладать только администратор безопасности;
- все неиспользуемые ресурсы операционной 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;
- исключить возможность удаленного изменения настроек ОС;
- установить атрибуты безопасности процессов и потоков в соответствии с требования безопасности всей системы в целом;
- отказаться от использования режима автоматического входа пользователя в операционную систему при ее загрузке;
- ограничить с учетом выбранной в организации политики безопасности использование пользователями запуска программ по расписанию;
- отключить сетевые протоколы, которые не используются на данной ЭВМ;
- запретить интерактивный вход пользователей через сеть;
- ограничить количество неудачных попыток входа в систему;
- использовать систему аудита, организовать регулярный анализ результатов аудита;
- настроить операционную систему на завершение работы при переполнении журнала аудита;
- необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):
  - файлы конфигураций;
  - файлы и каталоги;
  - временные файлы;
  - журналы системы;
  - файлы подкачки;
  - кэшируемая информация (пароли и т.п.);
  - отладочная информация;

- необходимо организовать затирание (по окончании сеанса работы ПБЗИ) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы ПБЗИ. Если это невыполнимо, 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.

- 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 ЭВМ с установленным ПБЗИ 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 на ЭВМ, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционирует ПБЗИ, и к компонентам ПБЗИ 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 и загруженной ключевой информацией нескольких пользователей.

### 4.3 Требования к работе с ключевой информацией

Создание, хранение, распределение, учет, использование и уничтожение ключевой информации, ключевых носителей и их архивных копий должно производиться в соответствии с разработанной в организации политикой управления ключевой информацией, являющейся составной частью политики безопасности организации.

В организации должен быть сотрудник (ответственный пользователь) за создание, хранение, распределение, учет, использование и уничтожение ключевой информации, ключевых носителей и их архивных копий. Должностные инструкции пользователей должны включать в себя порядок обращения с ключевой информацией. Необходимо также указать ответственность за ненадлежащее обращение с ключевой информацией, повлекшее за собой компрометацию ключей.

Ключевая информация (закрытые ключи подписи, шифрования и вычисления имитовектора) хранится в шифрованных на пароле пользователя ключевых контейнеров. Ключевые контейнеры рекомендуется хранить на съемных носителях (дискеты, USB Flash Hard Drive, CD и DVD диски) или в памяти аппаратных устройств (eToken производства компании «Aladdin Knowledge Systems Ltd», Rutoken производства компании «Актив», электронные таблетки Touch-Memory производства компании «Dallas Semiconductor» и т.д.).

Ключевые носители рекомендуется подключать к компьютеру только на время выполнения операций с ключами.

Все носители ключевой информации и их архивные копии подлежат поэкземплярному учету.

Режим хранения и использования ключей и их архивных копий должен исключить доступ к ним кого-либо, кроме владельца ключа, т.е. препятствовать компрометации ключей. В случае если компрометация произошла, необходимо гарантировать обнаружение этого факта.

При инициализации ПБЗИ начальное состояние ДСЧ необходимо вырабатывать с использованием биометрического датчика, входящего в состав ПБЗИ, или сертифицированным генератором (программным или аппаратно-программным), не входящем в состав ПБЗИ. При последующих инициализациях ПБЗИ начальное состояние ДСЧ, используемое для инициализации генератора случайных чисел может браться тремя способами:

- вырабатываться с использованием биометрического датчика, входящего в состав ПБЗИ;
- вырабатываться сертифицированным генератором (программным или аппаратно-программным), не входящим в состав ПБЗИ;
- (по умолчанию) в качестве начального берется ранее сохраненное состояние из специального контейнера ДСЧ, который, как и ключевой контейнер, защищен от модификации имитовектором и зашифрован.

По завершению работы с библиотекой в контейнер ДСЧ сохраняется текущее значение ДСЧ в качестве следующего начального.

Без инициализации ДСЧ работа ПБЗИ «Крипто-Си» Версия 2.0 невозможна.

Пользователь обязан:

- Не разглашать информацию о ключевых документах;
- Не допускать несанкционированное копирование ключевых документов
- Не передавать ключевые носители лицам, к ним не допущенным;
- Не выводить ключевую информацию на печатные устройства и дисплей;
- Не допускать записи на ключевой носитель посторонней информации;
- Не устанавливать ключевые носители в компьютеры, не входящие в состав программных и аппаратно-программных комплексов со встроенной в них ПБЗИ «Крипто-Си» Версия 2.

Рекомендуется регулярно проводить в организации проверку практического исполнения политики управления ключевой информацией.

Смена ключей подписи и шифрования должна производиться не реже, чем один раз в год.

Сроки уничтожения ключей и способ (физическое уничтожение ключевых носителей или путем стирания без повреждения ключевого носителя по технологии, обеспечивающей невозможность их восстановления) должны регламентироваться эксплуатационной и технической документацией. Факт уничтожения оформляется в соответствующих журналах поэкземплярного учета.

# 5. СКЗИ «ФОРОС. Исполнение №1»

## 5.1 Общие характеристики средств криптографической защиты СКЗИ ФОРОС 1

В СКЗИ ФОРОС 1 реализованы средства криптографической защиты информации на базе криптоалгоритмов по ГОСТ 28147-89, ГОСТ Р34.10-2001, ГОСТ Р34.11-94 которые обеспечивают:

- криптографическую аутентификацию карты внешним устройством;
- криптографическую аутентификацию внешнего устройства картой;
- взаимную криптографическую аутентификацию с выработкой сеансового ключа;
- возможность защищенного обмена данными с внешним устройством, при котором передаваемая информация шифруется на сеансовом ключе и защищается от искажений с помощью имитовставки;
- диверсификацию ключей
- выработку электронной цифровой подписи в соответствии с алгоритмом по ГОСТ Р34.10-2001;
- проверку электронной цифровой подписи в соответствии с алгоритмом по ГОСТ Р34.10-2001;
- выработку ключевой пары для алгоритма по ГОСТ Р34.10-2001;
- хеширование в соответствии с ГОСТ Р34.11-94;
- выработку псевдослучайных последовательностей.

Для реализации криптографических преобразований, в СКЗИ ФОРОС 1 встроен Криптомодуль, реализующий следующие функции:

- зашифрования/расшифрования области ОЗУ МК в соответствии с алгоритмом ГОСТ 28147-89 в режиме простой замены;
- зашифрования/расшифрования области ОЗУ МК в соответствии с алгоритмом ГОСТ 28147-89 в режиме гаммирования с обратной связью;
- зашифрования/расшифрования области ОЗУ МК в соответствии с алгоритмом ГОСТ 28147-89 в режиме простой замены с зацеплением;
- выработки имитовставки для области ОЗУ МК в соответствии с алгоритмом ГОСТ 28147-89 в режиме выработки имитовставки;
- диверсификации ключей;
- выработки электронной цифровой подписи в соответствии с алгоритмом по ГОСТ Р34.10-2001;

- проверки электронной цифровой подписи в соответствии с алгоритмом по ГОСТ Р34.10-2001;
- выработки ключевой пары для алгоритма по ГОСТ Р34.10-2001;
- хеширования в соответствии с ГОСТ Р34.11-94;
- выработки псевдослучайных последовательностей.

Функции криптомодуля используются средствами операционной системы при выполнении соответствующих команд и функций СКЗИ ФОРОС 1.

## 5.2 Условия эксплуатации СКЗИ ФОРОС 1

СКЗИ ФОРОС 1 предназначено для криптографической аутентификации МК со встроенным СКЗИ и внешних устройств, имитозащиты, шифрования и электронной подписи данных, передаваемых между МК и внешним устройством, а также для выработки ключей шифрования и электронной подписи.

СКЗИ ФОРОС 1 может быть использовано для шифрования конфиденциальной информации, не содержащей сведения, составляющих государственную тайну.

СКЗИ ФОРОС 1 может быть использовано для выработки электронной подписи информации, не содержащей сведения, составляющих государственную тайну.

После внесения криптографических ключей шифрования и электронной подписи в память МК, содержащего СКЗИ ФОРОС 1, ответственность за соблюдение организационных мер направленных на защиту ключевой информации в МК возлагается на лиц, ответственных за его эксплуатацию и хранение.

Срок действия криптографических ключей, используемых СКЗИ ФОРОС 1 не должен превышать 1 года.

Длительность 1 сеанса работы СКЗИ ФОРОС 1 должна быть ограничена 24 часами.

СКЗИ ФОРОС 1 сертифицировано ФСБ РФ по уровню "КС2" требований к средствам защиты конфиденциальной информации.

Заданный уровень защиты ("КС2") и подлинность передаваемой информации обеспечиваются при выполнении следующих условий:

- при применении функций криптографической защиты информации, в режимах предопределяющих использование криптографических функций;
- сохранение от компрометации ключевой информации;
- сохранение в тайне паролей пользователей.

В процессе эксплуатации МК содержащих СКЗИ ФОРОС 1 в составе средств, систем и комплексов, должны быть приняты меры по защите от использования посторонних устройств, эмулирующих работу МК с ОС СКЗИ ФОРОС 1 при выполнении рабочих транзакций.

В процессе эксплуатации МК содержащих СКЗИ ФОРОС 1 в составе средств, систем и комплексов, должны быть приняты меры по защите от использования посторонних устройств для подмены информации передаваемой между СКЗИ ФОРОС 1 и внешним устройством.

В процессе эксплуатации МК содержащих СКЗИ ФОРОС 1 в исполнении с бесконтактным или дуальным интерфейсом взаимодействия с внешними устройствами (терминальным

оборудованием), на расстоянии не менее 1-го метра должно быть исключено неконтролируемое пребывание посторонних лиц и транспортных средств.

Внешние устройства (терминалы), используемые для ввода ключевой информации в СКЗИ ФОРОС 1, а также обрабатывающие информацию, подлежащую защите от утечки по техническим каналам, должны быть аттестованы для обработки информации с ограниченным доступом (конфиденциальной информации) по действующим в Российской Федерации требованиям по защите информации по техническим каналам.

Для учета, хранения, транспортировки, уничтожения СКЗИ ФОРОС 1 должны быть разработаны правила и инструкции, учитывающие особенности использования МК в конкретных системах, комплексах и средствах.

Должны быть разработаны правила (инструкции) эксплуатации СКЗИ ФОРОС 1 для конкретных систем, комплексов или средств.