УТВЕРЖДЕНО

ИНФК.11485466.4012.027.31 01 ЛУ

Средство криптографической защиты информации "Бикрипт 5.0"

вариант исполнения 1 модификация 1, вариант исполнения 2 модификация 1, вариант исполнения 3 модификация 1, вариант исполнения 4 модификация 1, вариант исполнения 5 модификация 1, вариант исполнения 9 модификация 1, вариант исполнения 10 модификация 1, вариант исполнения 11 модификация 1

Правила пользования

ИНФК.11485466.4012.027.31 01

Листов 12

2018

1. Основные технические данные и характеристики СКЗИ

Настоящие Правила распространяются на модификацию 1 вариантов исполнений 1, 2, 3, 4, 5, 9, 10, 11 СКЗИ "Бикрипт 5.0".

СКЗИ "Бикрипт 5.0" представляет средство защиты конфиденциальной информации, удовлетворяющее:

- "Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений составляющих государственную тайну" для класса **КС1** в вариантах исполнения 1-5, "Требованиям к средствам электронной подписи" для класса **КС1** в вариантах исполнения 1-5;
- "Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений составляющих государственную тайну" для класса **КС2** в вариантах исполнения 9-11, "Требованиям к средствам электронной подписи" для класса **КС2** в вариантах исполнения 9-11 (отличающихся использованием сертифицированного по требованиям ФСБ России АПМДЗ, имеющего действующий сертификат соответствия.
- "Специальным требованиям к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведения, составляющих государственную тайну, и эксплуатируемых на территории Российской Федерации" по уровню КС во всех вариантах исполнений.

Средством СКЗИ "Бикрипт 5.0" **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

СКЗИ "Бикрипт 5.0" предназначено для эксплуатации под управлением операционных систем Windows XP, Windows Vista, Windows Server 2003/2008/2008 R2/2012/2012 R2/2016, Windows 7, Windows 8.1, Windows 10 (модификация 1 вариантов исполнений 1, 2, 9, 10), Linux (ядра 2.4, 2.6, 3.19, 4.4) (модификация 1 вариантов исполнений 3, 11), Solaris 11 (ядра 5.8, 5.9, 5.10, 5.11) (модификация 1 варианта исполнения 4), IBM Aix 7.1 (ядро 7) (модификация 1 варианта исполнения 5).

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 и ГОСТ Р 34.11-2012 "Информационная технология. Криптографическая защита информации. Функция хэширования".

Алгоритмы формирования и проверки ЭП реализованы в соответствии с требованиями ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".

Формирование электронной подписи по алгоритму ГОСТ Р 34.10-2001 после 31 декабря 2019 запрещается.

Алгоритм генерации пар открытый/закрытый ключи реализованы в соответствии с требованиями ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".

1.3. Требования к ПЭВМ

СКЗИ в вариантах исполнения 1, 2, 3, 9, 10, 11 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 9, 10, 11).

СКЗИ в варианте исполнения 4 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 5 должно функционировать на автономной ПЭВМ, оснащенной процессором не ниже IBM Power Systems POWER6, НЖМД емкостью не меньше 1 Гб, ОЗУ емкостью не меньше 1 Гб.

1.4. Съемные ключевые носители

К съемным ключевым носителям относятся: устройство "Touch Memory" DS1993 – DS1996; НГМД (3.5", 1.44 Mb); устройство VPN-Key (КД 11443195.4024-015, КД 11443195.4024-022); устройство USB FlashDrive.

1.5. Условные обозначения

АП – абонентский пункт, представляет собой СКЗИ "Бикрипт 5.0" модификация 1 вариантов исполнений 1, 2, 3, 4, 5, 9, 10 или 11.

2. Учет ключевой информации

2.1. Виды ключевой информации и ключевые носители

Название	Место создания	Область применения	Носитель
персональный ключ хранения (главный ключ)	АП	защита сетевых ключей и мастер-ключа АП	Съемный ключевой носитель
закрытый ключ ЭП	АП	формирование ЭП электронных документов	Съемный ключевой носитель
открытые ключи ЭП	АП	проверка ЭП электронных документов	Любой носитель
закрытый ключ шифрования	АП	шифрование сеансовых ключей	Съемный ключевой носитель
открытые ключи шифрования	АП	шифрование сеансовых ключей	Любой носитель
мастер-ключ ЭП (опционально)	АП	защита закрытых ключей ЭП пользователей	Любой носитель
ключ ПДСЧ	АП	генерация случайных последовательностей	Съемный ключевой носитель

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.

Допускается использование вместо съемных ключевых носителей неотчуждаемых носителей (например, НЖМД), при этом требования к ключевым носителям (п. 2.2) распространяются на системный блок ПЭВМ.

2.2. 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.

Системные блоки ПЭВМ с неотчуждаемыми носителями ключей, в том числе ключа ПДСЧ, следует хранить и эксплуатировать в специальных помещениях, размещение, специальное оборудование, охрана и организация режима в которых исключают доступ к системному блоку неуполномоченных лиц.

2.3. Сроки действия ключей

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

Допускается использование закрытых ключей ЭП для формирования ЭП на списки отозванных сертификатов в течение трех лет.

2.4. 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 СКЗИ "Бикрипт 5.0". Уничтожение ключевых носителей, за исключением НГМД, осуществляется путем расплющивания молотком на наковальне. НГМД уничтожаются путем оплавления до бесформенной массы.

2.5. Компрометация ключей

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

2.5.1. Компрометация закрытого ключа ЭП

При компрометации закрытого ключа ЭП предусматривается следующий порядок действий:

1. о факте компрометации немедленно ставятся в известность Администраторы всех АП-респондентов;

2. производится генерация новых ключей ЭП для данного пользователя и замена старого открытого ключа ЭП указанного пользователя на новый в справочниках (перерегистрация) на всех АП-респондентах, при использовании списка отозванных сертификатов, старый открытый ключ помещается в него и рассылается всем АП-респондентам;

3. скомпрометированный ключ ЭП в носителе уничтожается путем физического уничтожения ключевого носителя или записи на носитель нового закрытого ключа ЭЦП данного пользователя;

4. Администратор каждого АП-респондента принимает дополнительные меры по проверке подлинности документов с ЭП данного пользователя, которые были приняты АП с предполагаемого момента компрометации.

2.5.2. Компрометация закрытого ключа шифрования

При компрометации закрытого ключа шифрования предусматривается следующий порядок действий:

1. о факте компрометации немедленно ставятся в известность Администраторы всех АП-респондентов;

2. производится генерация новых ключей шифрования для данного пользователя и замена старого открытого ключа шифрования указанного пользователя на новый в справочниках (перерегистрация) на всех АП-респондентах;

3. скомпрометированный ключ шифрования в носителе уничтожается путем физического уничтожения ключевого носителя или записи на носитель нового закрытого ключа шифрования данного пользователя.

2.5.3. Компрометация мастер-ключа

В случае компрометации мастер-ключа предусматривается порядок действий аналогичный порядку, приведенному в п. 2.5.3 и 2.5.4.

3. Рекомендации по размещению технических средств с СКЗИ

При размещении технических средств с СКЗИ, следует руководствоваться следующими рекомендациями:

1. Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых установлены технические средства СКЗИ, 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 СКЗИ, радиотелефоны и другую радиоаппаратуру.

3. Должны выполняться требования политики безопасности, принятой в организации в области размещения технических средств, обрабатывающих конфиденциальную информацию.

4. СКЗИ "Бикрипт 5.0" необходимо устанавливать на ПЭВМ, разрешенные по требованиям информационной безопасности для обработки несекретной информации (конфиденциального характера), согласно принятой в информационной системе модели угроз (нарушителя).

5. Для обеспечения защиты опасных сигналов СКЗИ "Бикрипт 5.0" по уровню КС должны выполняться действующие в Российской Федерации требования по защите информации от утечки по техническим каналам, в том числе по каналу связи.

Защита линии связи, выходящей за пределы контролируемой зоны обеспечивается с использованием оптических медиаконвертеров, например, конвертора среды передачи интерфейса Fast Ethernet «ANCUD MC-FX/TX-100» фирмы "Анкад" (КБДЖ.467113.023 ТУ) или аналогичных.

В соответствии с Требованиями Положения ПКЗ-2005 данные требования необходимо выполнять в следующих случаях:

- если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации;

- при организации криптографической защиты информации конфиденциального характера в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации;

- при организации криптографической защиты информации конфиденциального характера в организациях независимо от их организационно-правовой формы и формы собственности при выполнении ими заказов на поставку товаров, выполнение работ или оказание услуг для государственных нужд;

- если обязательность защиты информации конфиденциального характера возлагается законодательством Российской Федерации на лиц, имеющих доступ к этой информации или наделенных полномочиями по распоряжению сведениями, содержащимися в данной информации;

- при обрабатывании информации конфиденциального характера, обладателем которой являются государственные органы или организации, выполняющие государственные заказы, в случае принятия ими мер по охране ее конфиденциальности путем использования средств криптографической защиты;

- при обрабатывании информации конфиденциального характера в государственных органах и в организациях, выполняющих государственные заказы, обладатель которой принимает меры к охране ее конфиденциальности путем установления необходимости криптографической защиты данной информации.

Данные требования носят рекомендательный характер при эксплуатации СКЗИ "Бикрипт 5.0" для защиты информации:

- доступ к которой ограничивается по решению обладателя, пользователя (потребителя) данной информации, собственника (владельца) информационных ресурсов (информационных систем) или уполномоченных ими лиц, не являющихся государственными органами или организациями, выполняющими государственные заказы;

- открытых и общедоступных государственных информационных ресурсов Российской Федерации.

6. 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 СКЗИ "Бикрипт 5.0", должно использоваться только лицензионное программное обеспечение фирм-производителей, либо ПО, сертифицированное ФСБ. Указанное ПО не должно содержать средств разработки и отладки приложений, а также содержать в себе возможностей, позволяющих оказывать воздействие на функционирование СКЗИ. 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 разрешенная операционная система.

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. В BIOS ПЭВМ определяются установки, запрещающие удаленное управление ПЭВМ при его наличии. Не применяются ПЭВМ с BIOS, исключающим возможность отключения удаленного управления.

5. Средствами BIOS должна быть исключена возможность использования пользователем "горячих" клавиш для активации или отключения встроенных функциональных возможностей ПО BIOS.

6. Средствами BIOS должна быть исключена возможность отключения пользователями устройств АПМДЗ и СЗИ, манипулирования критическими параметрами СВТ, загрузки нештатных копий ОС, перепрограммирования микросхем ППЗУ с ПО BIOS.

7. 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.

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

9. Программные модули СКЗИ (прикладного ПО со встроенным СКЗИ) должны быть доступны только по чтению/запуску (в атрибутах файлов запрещена запись и модификация).

10. Администратором безопасности должно быть проведено опечатывание системного блока с установленным СКЗИ, исключающее возможность несанкционированного изменения аппаратной части рабочей станции.

11. При эксплуатации АПМДЗ в составе СКЗИ, должны выполняться требования, изложенные в нормативных документах, входящих в состав АПМДЗ, указанного в формуляре.

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

СКЗИ "Бикрипт 5.0" при условии выполнения настоящих Правил обеспечивает защиту конфиденциальной информации по уровню КС1 для вариантов исполнения 1-5 и по уровню КС2 - для вариантов исполнения 9-11.

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 СКЗИ "Бикрипт 5.0" следует принять следующие организационные меры:

1. Право доступа к рабочим местам с установленным ПО СКЗИ "Бикрипт 5.0" должно предоставляться только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на программное обеспечение, имеющее в своем составе СКЗИ "Бикрипт 5.0".

2. Запретить осуществление несанкционированного администратором безопасности копирования ключевых носителей.

3. Запретить передачу ключевых носителей лицам, к ним не допущенным.

4. Запретить использование ключевых носителей в режимах, не предусмотренных правилами пользования СКЗИ "Бикрипт 5.0", 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 СКЗИ "Бикрипт 5.0" 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 hashctrl, входящей в состав СКЗИ (см. Приложение 1).

2. При каждом запуске ПЭВМ с установленным ПО СКЗИ должен осуществляться контроль целостности программного обеспечения, входящего в состав СКЗИ "Бикрипт 5.0", самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ. При использовании СКЗИ в вариантах исполнения 1-5, контроль должен осуществляться утилитой hashctrl, входящей в состав СКЗИ, в вариантах исполнения 9-11 - средствами АПМДЗ.

3. В вариантах исполнений 9-11 дополнительно средствами АПМДЗ должен осуществляться контроль целостности открытых ключей, хранящихся на НЖМД АП.

4. Администратор должен периодически (не реже 1 раза в год) менять пароль на вход в BIOS.

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

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

7. При использовании СКЗИ в варианте исполнения 1-5 средствами BIOS или ОС для пользователя должен быть установлен пароль входа в систему длиной не менее 6 символов, в варианте исполнения 9-11 – идентификация и аутентификация должны производиться средствами АПМДЗ, указанном в формуляре. Пароль или идентификатор должен меняться не реже 1 раза в год. Число попыток ввода пароля одним пользователем не должно превышать 10 раз. 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 ПЭВМ должна быть установлена только одна операционная система.
- Правом установки и настройки ОС и СКЗИ должен обладать только администратор безопасности.
- ОС должна быть настроена только для работы с СКЗИ. 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 НЖМД 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.

• Должны использоваться антивирусные средства;

• Необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы.

• В случае подключения ПЭВМ с установленным СКЗИ 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 СКЗИ 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 СКЗИ, и к компонентам СКЗИ 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.

• При эксплуатации СКЗИ под управлением ОС Windows 10/Windows Server 16 необходимо отключить функции телеметрии следующим образом:

1. Проверить наличие и статус сервиса DiagTrack (Панель управления -> Система и безопасность -> Администрирование -> Службы).
2. Если сервис запущен, то остановить его.
3. Удалить запись регистрации сервиса DiagTrack из реестра (Пуск -> выполнить -> regedit, раздел HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services (найти и удалить папку DiagTrack).
4. Удалить подготовленные к отправке данные, которые сохраняются в файлах с расширением *.rbs, хранящихся в директории %ProgramData%\Microsoft\Diagnosis. Необходимо удалить все файлы с расширением *.rbs. При возникновении проблем с удалением указанных файлов необходимо предварительно в свойствах на вкладке "Безопасность" разрешить полный доступ к файлам, а затем удалить их.
5. Остановить автоматическую (AutoLogger) ETW сессию AutoLogger-DiagTrack-Listener, которую DiagTrack активирует в процессе своей остановки.
6. Удалить файл, в который автоматическая (AutoLogger) ETW сессия AutoLogger-DiagTrack-Listener сохраняла собранные данные. Путь к файлу хранится в реестровой записи AutoLogger-DiagTrack-Listener в значении FileName. Конфигурации автоматических (AutoLogger) ETW сессий находятся в ключе реестра HKLM\SYSTEM\CurrentControlSet\Control\WMI\AutoLogger. Конфигурация целевой сессии хранится в данном ключе под записью AutoLogger-DiagTrack-Listener.
В настоящее время данные сохраняются в файл
%ProgramData%\Microsoft\Diagnosis\ETLLogs\AutoLogger\AutoLogger-DiagTrack-Listener.etl.
7. Удалить запись регистрации конфигурации автоматической (AutoLogger) ETW сессии AutoLogger-DiagTrack-Listener из реестра.

Данные действия необходимо выполнять после каждого кумулятивного обновления, поскольку при таких обновлениях удаленные сервисы восстанавливаются.

6.4. Требования по встраиванию СКЗИ в приложения

Разработка прикладного программного обеспечения на основе вариантов исполнений 1, 2, 3, 4, 5, 9, 10, 11 СКЗИ "Бикрипт 5.0" может производиться без создания новых СКЗИ и без проведения тематических исследований в случае использования вызовов из функций, описанных в приложении 2 к настоящим Правилам пользования.

В случае использования прочих вызовов необходимо производить разработку отдельного варианта исполнения СКЗИ или нового СКЗИ в соответствии с действующей нормативной базой (в частности, с Постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313 и Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)).

Прикладное программное обеспечение должно анализировать коды возврата функций библиотеки и прекращать выполнение операции при ошибочном коде возврата.

При использовании функций шифрования необходимо выполнять следующие требования:

• не использовать алгоритмы выработки ключей (включая алгоритмы ключевого обмена) отличные от описанных в Инструкции программиста ИНФК.11485466.4012.027.32 01;

• при использовании режимов шифрования, требующих синхропосылки, применять протоколы, обеспечивающие надежную (без искажений) передачу синхропосылки получателю; необходимо

также обеспечить защиту от повторного использования синхропосылки с одним и тем же ключом шифрования;

• перед зашифрованием сообщение должно быть подписано электронной подписью, которая должна быть проверена после расшифрования;

• уничтожать контекст шифрования сразу после использования.

При использовании функций, реализующих алгоритмы электронной подписи, необходимо выполнять следующие требования:

• при распространении открытых ключей ЭП применять методы, обеспечивающие целостность открытых ключей и аутентификацию их владельцев;

• при выработке/проверке подписи использовать функции хеширования данных, реализованные в СКЗИ "Бикрипт 5.0";

• при проведении процедур проверки электронной подписи выполнять аутентификацию владельца открытого ключа, а также проверку целостности и действительности ключа на момент проверки;

• уничтожать контекст подписи сразу после использования.

При использовании функций, реализующих алгоритмы ключевого обмена, необходимо выполнять следующие требования:

• при распространении открытых ключей шифрования применять методы, обеспечивающие целостность открытых ключей и аутентификацию их владельцев;

• необходимо применять меры, обеспечивающие аутентификацию общего ключа шифрования, выработанного с помощью процедур ключевого обмена (для исключения атаки man-in-the-middle);

• использовать меры, предотвращающие повторение ранее выполненных процедур ключевого обмена;

• уничтожать контекст ключевого обмена сразу после использования.

При использовании СКЗИ "Бикрипт 5.0" в системах без автоматического создания и (или) автоматической проверки ЭП ПО, использующее библиотеки СКЗИ "Бикрипт 5.0" 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:

• 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.

Приложение 1.

Контроль целостности программного обеспечения

Для обеспечения возможности контроля целостности программных модулей (файлов) запуск программы hashctrl должен осуществляться с аргументами командной строки:

Без параметров – на экран выведется окно со списком допустимых параметров.
hashctrl [options] [path+mask] [outfile]
Если задан параметр [outfile], то вывод программы выдается в outfile
Опции:
/h0 - набор параметров соответствует примеру в тексте ГОСТ Р 34.11-94
/h1 - при расчете значения хеш-функции используется набор параметров СКЗИ "Бикрипт-КСБ-М"
/h2 - при расчете значения хеш-функции используется набор параметров СКЗИ "Бикрипт 4.0" и "CryptoPro CSP" (параметр используется по умолчанию)
/h3 - набор параметров соответствует применяемому в модуле контроля целостности WinFPSUhash.exe
/h256 - набор параметров соответствует ГОСТ 34.11-2012 256-бит СКЗИ "Бикрипт 5.0"
/h512 - набор параметров соответствует ГОСТ 34.11-2012 512-бит СКЗИ "Бикрипт 5.0"
/p1 - печать значений, как в тестовом примере ГОСТ Р 34.11-94
/p2 - печать значений производится слитно, от младших байт к старшим (параметр используется по умолчанию)
/l:<filelist> - в качестве входного потока имен файлов используется список файлов в <filelist> (если не задан, то используется hash.lst)
/m - список файлов в параметре [path+mask] или /l:<filelist> рассматривается программой как единый масив данных для расчета потокового хеша (аналог утилиты ashdir.exe)
/r - рекурсивный обход каталогов начиная с текущего или указанного в параметре [path+mask]. Параметр не совместим с параметром /l

Примеры запуска:
Чтобы вычислить хеш для всех файлов в текущей директории и записать результат в файл result.hsh:
hashctrl *.* result.hsh
Чтобы вычислить поточный (общий) хеш для всех файлов в текущей директории как в тексте ГОСТ Р 34.11-94:
hashctrl /m *.* /h0 /p1

/calc - вычислить хэш для каждого файла из последующего списка (значение хэша записывается в файл FileName.hsh)
/check - проверить хэш для каждого файла из последующего списка (значение хэша считывается из файла FileName.hsh) (если хэш верен, то выйти без сообщения если не задано /info; если хэш неверен - сообщение об этом выдается всегда)
/info - проверить хэш и выдать сообщение о результатах проверки

Примеры запуска:
Записать хэш файла testfile.txt в файл testfile.txt.hsh:
hashctrl /calc testfile.txt

Проверить хэш файла testfile.txt (при этом требуется файл testfile.txt.hsh):
hashctrl /info testfile.txt

Проверить хэш файла testfile.txt без выдачи сообщения о правильном хэше:
hashctrl /check testfile.txt

Если в результате контроля целостности при загрузке операционной системы появляется сообщения о нарушении целостности контролируемого файла, пользователь обязан прекратить работу и обратиться к администратору безопасности.

Администратор безопасности, проанализировав причину, приведшую к нарушению целостности, должен переустановить ПО СКЗИ "Бикрипт 5.0", или файлы операционной среды.

Приложение 2.

Перечень вызовов, использование которых при разработке прикладного ПО с применением СКЗИ "Бикрипт 5.0" возможно без проведения дополнительных тематических исследований.

Функция	Описание
cr_GetNextByStorage	Получение следующего индекса цепочки сертификатов
cr_GetRootByStorage	Получение корневого сертификата в цепочке сертификатов
cr_GetFilenameByStorage	Получение имени файла сертификата в хранилище
cr_GetBufferByStorage	Получение сертификата из хранилища
cr_GetStatusByStorage	Получение статуса сертификата из хранилища
cr_GetChainSizeByStorage	Получение длины цепочки сертификатов в хранилище
cr_GetStorageInfo	Получение количества сертификатов и списка отозванных сертификатов в хранилище
cr_CreateTime	Создание контекста времени
cr_FreeTime	Освобождение контекста времени
cr_SetCurrentTime	Установка текущего времени для контекста времени
cr_SetTime	Установка заданного времени в контекст
cr_GetTime	Получение времени из контекста
cr_CopyTime	Копирование контекста времени
cr_GetCertificateUsageInfo	Политика сертификата и класс средства ЭП
cr_DeleteSignBuffer	Удаление ЭП из CMS
cr_GetCmsData	Получение информации об ЭП из CMS в буфере
cr_GetFileData	Получение информации об ЭП из CMS в файле
cr_GetCmsTimeCn	Получение времени ЭП и выделенного имени подписанта CMS в буфере
cr_GetCmsFileTimeCn	Получение времени ЭП и выделенного имени подписанта CMS в файле
cr_GetCrlTimeCn	Получение времени ЭП и выделенного имени создателя списка отозванных сертификатов
cr_GetCertificateTimeCn	Получение времени ЭП и выделенного имени владельца из сертификата в буфере
cr_GetCertificateTimeCnByStorage	Получение времени ЭП и выделенного имени владельца из сертификата в хранилище
cr_Finalize	Завершение работы
cr_GenerateKeyPair	Создание ключевой пары на основе выделенного имени и атрибутов, кодированных в формате ASN.1
cr_GenerateKeyPairByQualNames	Создание ключевой пары на основе данных, идентифицирующих владельца сертификата
cr_CreateContext	Инициализация контекста библиотеки
cr_AddCertificate	Добавление сертификата в контекст библиотеки
cr_AddCrl	Добавление списка отозванных сертификатов в контекст библиотеки
cr_AddCertificateAndCrlByPath	Добавление сертификатов и списков отозванных сертификатов из файлов в контекст библиотеки
cr_LoadPrnd	Инициализация датчика ПДСЧ
cr_DupContext	Создание копии контекста библиотеки
cr_FreeContext	Освобождение контекста библиотеки
cr_GetNumOfKeyPair	Получение количества ключевых пар в контексте библиотеки
cr_GetKeyPairInfo	Получение информации о ключевой паре в контексте библиотеки
cr_GetPrndCarrier	Получение информации о носителе ключа ПДСЧ в контексте библиотеки
cr_FindKeyPair	Поиск ключевой пары по сертификату в контексте библиотеки
cr_LoadKeyPair	Загрузка ключевой пары в контексте библиотеки
cr_FreeKeyPair	Освобождение ресурсов ключевой пары
cr_DigestInit	Инициализация контекста вычисления значений хеш-функции
cr_SetDigestParam	Задание параметров контекста вычисления значений хеш-функции
cr_SetDigestParamByKeyPair	Задание параметров контекста вычисления значений хеш-функции, согласованных с ключевой парой
cr_DigestBuffer	Получение значения хеш-функции для буфера памяти
cr_DigestUpdate	Добавление порции данных в контекст вычисления значений хеш-функции
cr_DigestFinal	Получение значения в контексте вычисления значений хеш-функции

cr_DigestClose	Закрыть контекст вычисления значений хеш-функции
cr_SignInit	Инициализация контекста операции формирования ЭП
cr_SignPutHash	Добавление значения хеш-функции в контекст операции формирования ЭП
cr_SignPutData	Накопление данных в контексте операции формирования ЭП
cr_SignPutCms	Добавление в контекст операции формирования ЭП существующей CMS
cr_Sign	Формирование ЭП в контексте операции формирования ЭП
cr_SignClose	Закрытие контекста операции формирования ЭП
cr_SignBuffer	Электронная подпись области памяти
cr_SignFile	Электронная подпись файла
cr_SignHash	Электронная подпись значения хеш-функции
cr_CheckInit	Инициализация контекста операции проверки ЭП
cr_CheckPutHash	Добавление значения хеш-функции в контекст операции проверки ЭП
cr_CheckPutData	Накопление данных для проверки отсоединенной ЭП в контексте операции проверки ЭП
cr_CheckPutCms	Добавление в контекст операции проверки ЭП существующей CMS
cr_Check	Проверка ЭП и получение результатов в контексте операции проверки ЭП
cr_CheckClose	Закрытие контекста операции проверки ЭП
cr_CheckBuffer	Проверка ЭП области памяти
cr_CheckBuffer2	Проверка ЭП области памяти
cr_CheckFile	Проверка ЭП файла
cr_CheckFile2	Проверка ЭП файла
cr_CheckHash	Проверка ЭП значения хеш-функции
cr_CheckCertificateByStorage	Проверка ЭП сертификата из хранилища
cr_CheckCertificate	Проверка ЭП сертификата из буфера по хранилищу
cr_CheckPKCS10	Проверка ЭП запроса на сертификат
cr_CheckCrl	Проверка ЭП списка отозванных сертификатов по хранилищу
cr_EncryptInit	Инициализация контекста операции зашифрования
cr_EncryptPutData	Накопление данных в контексте операции зашифрования
cr_Encrypt	Выполнение шифрования блока данных в контексте операции зашифрования Примечание: допустимо шифрование только предварительно подписанных функциями СКЗИ данных.
cr_EncryptClose	Закрытие контекста операции зашифрования
cr_EncryptBuffer	Зашифрование области памяти Примечание: допустимо шифрование только предварительно подписанной функциями СКЗИ области памяти.
cr_DecryptInit	Инициализация контекста операции расшифрования
cr_DecryptPutEnvelopedCms	Добавление в контекст операции расшифрования существующей CMS
cr_Decrypt	Выполнение расшифрования блока данных в контексте операции расшифрования Примечание: данные считаются правильно расшифрованными только при положительном результате проверки электронной подписи на данные функциями СКЗИ.
cr_DecryptClose	Закрытие контекста операции расшифрования
cr_DecryptBuffer	Расшифрование области памяти Примечание: область памяти считается правильно расшифрованной только при положительном результате проверки электронной подписи на область памяти функциями СКЗИ.
ConfirmCertReq	Создание подписанного CMS с PKCS#10 запросом внутри
IssueCertificate	Создание сертификата на основе запроса и подпись его ключом пользователя
IssueRootCertificate	Создание корневого сертификата
CreateKeyPairFromBicrKey	Создание ключевой пары администратора ЦС на основе ключа в формате БиКрипт
CreateCrl	Создание Списка отзыва и подпись его ключом пользователя
cr_CreateCarrierGUI	Создание контекста пути доступа к закрытому ключу
cr_FreeCarrier	Освобождение контекста пути доступа к закрытому ключу
cfg	Вызов конфигуратора