КРИПТОКОМ

УТВЕРЖДЕН
СЕИУ.00009-03 94 - ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
МагПро КриптоПакет вер. 2.1

Правила эксплуатации

СЕИУ.00009-03 94
Листов 20

Литера О

2012

Аннотация

Настоящий документ регламентирует правила эксплуатации программных компонентов средства криптографической защиты информации (СКЗИ) «МагПро КриптоПакет» в. 2.1.

Содержание

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

1 Требования к пользователям СКЗИ.

В организации, эксплуатирующей СКЗИ, должен быть назначен администратор безопасности, на которого возлагаются задачи организации работ по использованию СКЗИ, выработки соответствующих инструкций для пользователей, а также контроль за соблюдением приведенных требований.

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

Пользователь СКЗИ должен принять на себя обязательства по нераспространению доверенных ему конфиденциальных сведений (в частности, ключевой информации). Такие обязательства могут включаться непосредственно в текст контракта (договора). Пользователь допускается к работе с СКЗИ после подписания обязательств, определяющих его материальную или иную форму ответственности за возможные нарушения.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

2 Требования к объектам размещения СКЗИ.

Эксплуатация СКЗИ разрешается только на территории Российской Федерации.

При размещении технических средств с установленным СКЗИ 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.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

3 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.

На технических средствах, предназначенных для работы с СКЗИ, должно использоваться только лицензионное программное обеспечение фирм-изготовителей.

Подключаемое к ПЭВМ оборудование не должно создавать угроз безопасности ОС и СКЗИ, установленных на ПЭВМ.

ПЭВМ, на которой устанавливается СКЗИ, должна выполнять процедуры самоконтроля основных аппаратных компонентов после каждого сброса системы, включая момент появления питания. Регламент использования ПЭВМ должен предусматривать перезакрузку ПЭВМ не реже одного раза в неделю.

Установка ПО СКЗИ должна производиться только лицами, имеющими допуск к работам в соответствии с нормами безопасности, принятыми в организации.

Установка ПО СКЗИ на ПЭВМ должна производиться только с зарегистрированного, защищенного от записи лицензионного носителя.

Совместно с СКЗИ должны использоваться средства антивирусной защиты, сертифицированные по требованиям ФСБ России. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.

На ПЭВМ 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 или иным должностным лицом, ответственным за обеспечение информационной безопасности в организации. 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.

Программное обеспечение, устанавливаемое на ПЭВМ 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;
- использовать недокументированные фирмой-разработчиком функции ОС.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

4 Требования по организации контроля целостности.

Должны быть предусмотрены меры, исключающие возможность несанкционированного необнаруживаемого изменения аппаратной части технических средств, на которых установлено СКЗИ (например, путем опечатывания системного блока и разъемов ПЭВМ).

Должен осуществляться периодический (не реже раза в неделю) контроль целостности установленного ПО СКЗИ, а также его окружения. Контроль целостности обеспечивается программными средствами путем вычисления хэш-векторов файлов и сравнения вычисленных хэш-векторов с эталонными значениями.

Перечень модулей СКЗИ, подлежащих контролю целостности, и значения хэш-векторов для них приведены в формуляре на СКЗИ.

Для операционных систем Windows перечень системных модулей и ключей реестра, подлежащих контролю целостности, приведен в Приложении, вычисление значений хэш-векторов осуществляется программой calchash, входящей в состав СКЗИ.

Для остальных операционных систем контроль целостности осуществляется с помощью средства контроля целостности integrity, входящего в состав СКЗИ. Средство integrity автоматически определяет перечень системных модулей, влияющих на правильность работы СКЗИ, и вычисляет значения хэш-векторов этих модулей.

Эталонные значения хэш-векторов модулей операционной системы должны быть вычислены при установке СКЗИ. После установки обновлений операционной системы эталонные значения обновленных модулей должны быть перевычислены. При формировании файла эталонных значений хэш-векторов необходимо убедиться в совпадении хэш-векторов для модулей СКЗИ с зафиксированными в формуляре на СКЗИ.

Файл эталонных значений хэш-векторов должен храниться на отчуждаемом носителе наравне с ключевой информацией. При осуществлении периодического контроля целостности этот файл должен быть доступен в режиме «только чтение» (компакт-диск, дискета с защитой от записи и т.п.).

При выявлении нарушений целостности модулей СКЗИ или операционной системы необходимо выявить и устранить причины искажения модулей.

Восстановление целостности СКЗИ осуществляется с помощью средств установки СКЗИ или программного комплекса, использующего СКЗИ:

- для Windows – путем повторной установки СКЗИ;
- для unix-подобных ОС – путем повторной установки пакета в режиме «reinstall».

Перед установкой СКЗИ необходимо проверить целостность дистрибутивных пакетов СКЗИ (перечень дистрибутивных пакетов и значения хэш-векторов для них приведены в формуляре на СКЗИ).

Восстановление целостности операционной системы осуществляется в соответствии с рекомендациями ее разработчика.

По завершении процедур восстановления целостности модулей СКЗИ и/или операционной системы должна быть проведена проверка коррекности восстановления путем вычисления хэш-векторов модулей и их сравнения с ранее зафиксированными эталонными значениями.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

5 Требования по организации защиты от несанкционированного доступа.

Защита аппаратного и программного обеспечения от несанкционированного доступа (НСД) при установке и использовании СКЗИ 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.

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 администратором безопасности.

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;
- 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.п.);
- 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.

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.

При использовании СКЗИ совместно с АПМДЗ средствами используемого АПМДЗ должна быть обеспечена аутентификация пользователя до загрузки ОС.[1] При этом необходимо организационно запретить сотрудникам, эксплуатирующим СКЗИ, оставлять без присмотра во включенном состоянии ПЭВМ, на которой установлена СКЗИ.

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

[1]См.«Руководство администратора АПМДЗ «Аккорд-АМДЗ»», разделы 1.5-1.7, либо «Руководство по администрированию программно-аппаратного комплекса «Соболь»», глава 3, раздел «Управление пользователями».

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

На ПЭВМ должна быть установлена только одна операционная система. Правом установки и настройки ОС и СКЗИ должен обладать только администратор безопасности.

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;
- отключить все неиспользуемые ресурсы системы (протоколы, сервисы и т.п.);
- настроить на максимальный уровень все режимы безопасности, реализованные в ОС;
- назначить минимально возможные для нормальной работы права всем пользователям и группам, зарегистрированным в 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;
- ограничить количество неудачных попыток входа в систему.

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.

Необходимо исключить одновременную работу в ОС с работающим СКЗИ и загруженной ключевой информацией нескольких пользователей.

Должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии. В частности, необходимо организовать и использовать комплекс мероприятий антивирусной защиты.

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.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

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 и т.п.), 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.

Необходимо организовать и использовать систему аудита, организовать регулярный анализ результатов аудита. Необходимо настроить операционную систему на завершение работы при переполнении журнала аудита.

Запрещается оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации либо иной конфиденциальной информации.

Запрещается вносить какие-либо изменения в программное обеспечение СКЗИ.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

6 Требования по защите от утечки информации по каналам ПЭМИН

Если модель угроз в информационной системе Заказчика предполагает защиту информации, обрабатываемой с использованием СКЗИ, от утечки по техническим каналам, в том числе по каналу связи, ПЭВМ, на которых предполагается эксплуатация СКЗИ, должны быть допущены для обработки конфиденциальной информации по действующим в Российской Федерации требованиям по защите от утечки по техническим каналам (например, СТР-К).

В случае планирования размещения ПЭВМ с СКЗИ в помещениях, где присутствует речевая акустическая информация, содержащая сведения, составляющие государственную тайну, ПЭВМ должны быть подвергнуты специальной проверке по выявлению устройств, предназначенных для негласного получения информации, а также специсследованиям на соответствие требованиям к вычислительной технике средств связи по защите от утечки информации по каналам ПЭМИН в соответствии с категорией выделенного помещения.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

7 Требования к работе с ключевой информацией.

Закрытый ключ пользователя должен размещаться на отчуждаемом носителе (далее по тексту именуемом ключевым носителем). Ключевой носитель должен быть доступен только специально уполномоченному на это сотруднику (владельцу ключей).

В случае, если необходимо загрузить ключи в приложение на сервере, к которому невозможно подключить ключевой носитель (ввиду отсутствия физического доступа владельца ключа к серверу или иных причин), в порядке исключения допускается удаленная загрузка закрытого ключа по сети с рабочего места владельца ключа. При этом должны быть выполнены следующие условия:

- на рабочее место владельца ключа должно быть установлено СКЗИ «МагПро КриптоПакет» в. 2.1 с полным соблюдениме требований, предъявляемых настоящими «Правилами эксплуатации»;
- на рабочем месте владельца ключа файл закрытого ключа должен быть зачитан в область оперативной памяти, зашифрован средствами СКЗИ «МагПро КриптоПакет» в. 2.1 и передан на сервер, после чего использованную область оперативной памяти необходимо затереть;
- на сервере принятый файл закрытого ключа должен быть записан в область оперативной памяти, там расшифрован средствами СКЗИ «МагПро КриптоПакет» в. 2.1 и загружен в приложение, после чего использованную область оперативной памяти необходимо затереть;
- недопустима запись закрытого ключа в какие-либо временные файлы как на рабочем месте владельца ключа, так и на сервере.

Примечание. При использовании СКЗИ для защиты информации в серверных приложениях допускается также размещение закрытого ключа на жестком диске компьютера. При этом режим хранения и использования компьютера должен обеспечивать выполнение требований по работе с ключевой информацией, указанных в настоящем разделе.

После выработки, но до ввода в эксплуатацию открытый ключ должен пройти обязательную сертификацию в Удостоверяющем Центре, сертифицированном по классу не ниже уровня защиты СКЗИ, либо средствами самого СКЗИ. Кроме того, пользователь или администратор безопасности (при наличии в организации, эксплуатирующей СКЗИ) должен своевременно выводить из действия ключевые пары по истечению срока годности или при компрометации закрытого ключа.

Файлы сертификатов открытых ключей и списков отзыва не содержат закрытой информации и могут располагаться на жестком диске компьютера. При этом должна быть обеспечена защита корневых сертификатов от искажения и подмены.

При каждом использовании сертификата ключа подписи или ключа обмена должна проводиться проверка сертификата с помощью открытого ключа подписи УЦ и проверка, что данный сертификат не является отозванным.

В случае повреждения или уничтожения ключевого носителя в результате программных и аппаратных сбоев, несчастных случаев и т.п. работоспособность «МагПро КриптоПакет» в. 2.1 будет нарушена. Для возможности максимально быстрого и полного восстановления работоспособности комплекса в подобных ситуациях рекомендуется заблаговременно создавать архивную копию закрытого ключа на резервном ключевом носителе. При этом режим создания и хранения архивных копий должен исключать доступ к этим копиям кого-либо, кроме владельца ключа.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Архивную копию закрытого ключа на резервном носителе рекомендуется создавать сразу по завершении процедуры создания новых ключей или смены ключей.

При создании новых архивных копий предыдущие (ставшие неактуальными) архивные копии должны быть уничтожены. Ключевые носители после удаления с них закрытого ключа и его архивных копий должны использоваться в том же качестве (для хранения новых ключей) либо уничтожаться.

Все ключевые носители и их архивные копии подлежат строгому поэкземплярному учету.

Создание, хранение, использование и уничтожение выведенной из использования ключевой информации должно производится строго в соответствии с должностной инструкцией.

Смена ключей должна производиться в сроки, определенные должностной инструкцией, но не реже одного раза в год.

Режим хранения и использования ключевых носителей должен максимально препятствовать компрометации ключей, то есть доступу к ключевому носителю посторонних лиц, либо возникновению условий, при которых такой доступ был возможен. В случае, если компрометация все же произошла, режим хранения и использования ключевых носителей должен гарантировать обнаружение этого факта.

Пользователь несет персональную ответственность за соблюдение режима хранения и использования своих ключевых носителей, в том числе при транспортировке ключевых документов из УЦ до ПЭВМ. О фактах компрометации ключевой информации пользователь должен немедленно поставить в известность ответственных лиц и действовать в соответствии с должностной инструкцией.

Запрещается:

- 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.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

8 ПРИЛОЖЕНИЕ. Перечень модулей СКЗИ, модулей и ключей реестра операционной системы Windows, подлежащих контролю целостности

Перечень модулей СКЗИ для операционной системы Windows, подлежащих контролю целостности:

cryptocom.dll
libeay32.dll
ssleay32.dll
openssl.exe
calchash.exe

Перечень модулей СКЗИ для операционных систем Linux, FreeBSD, Sun Solaris, подлежащих контролю целостности:

libcryptocom.so
libcrypto.so.1.0.0
libssl.so.1.0.0
openssl
calchash
gostsum
skcs

Перечень исполняемых модулей операционной системы Windows, подлежащих контролю целостности:

\windows\apppatch\acgenral.dll
\windows\explorer.exe
\windows\system32\activeds.dll
\windows\system32\actxprxy.dll
\windows\system32\adsldpc.dll
\windows\system32\advapi32.dll
\windows\system32\advpack.dll
\windows\system32\alg.exe
\windows\system32\apphelp.dll
\windows\system32\atl.dll
\windows\system32\audiosrv.dll
\windows\system32\authz.dll
\windows\system32\autochk.exe
\windows\system32\basesrv.dll
\windows\system32\batmeter.dll
\windows\system32\bootvid.dll
\windows\system32\browser.dll
\windows\system32\browseui.dll
\windows\system32\cabinet.dll
\windows\system32\certcli.dll
\windows\system32\clbcatq.dll

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

\windows\system32\clusapi.dll
\windows\system32\cnbjmon.dll
\windows\system32\colbact.dll
\windows\system32\comctl32.dll
\windows\system32\comdlg32.dll
\windows\system32\comres.dll
\windows\system32\comsvcs.dll
\windows\system32\credui.dll
\windows\system32\crypt32.dll
\windows\system32\cryptdll.dll
\windows\system32\cryptsvc.dll
\windows\system32\cryptui.dll
\windows\system32\cscdll.dll
\windows\system32\cscui.dll
\windows\system32\csrsrv.dll
\windows\system32\csrss.exe
\windows\system32\ctfrnon.exe
\windows\system32\davclnt.dll
\windows\system32\dhcpcsvc.dll
\windows\system32\dmserver.dll
\windows\system32\dmusic.dll
\windows\system32\dnsapi.dll
\windows\system32\dnsrslvr.dll
\windows\system32\dpcdll.dll
\windows\system32\drprov.dll
\windows\system32\dssenh.dll
\windows\system32\ersvc.dll
\windows\system32\es.dll
\windows\system32\esent.dll
\windows\system32\eventlog.dll
\windows\system32\framebuf.dll
\windows\system32\gdi32.dll
\windows\system32\hal.dll
\windows\system32\hnetcfg.dll
\windows\system32\icaapi.dll
\windows\system32\icmp.dll
\windows\system32\imagehlp.dll
\windows\system32\imapi.exe
\windows\system32\inetpp.dll
\windows\system32\iphlpapi.dll
\windows\system32\ipnathlp.dll
\windows\system32\kbdru.dll
\windows\system32\kbdus.dll
\windows\system32\kdcom.dll
\windows\system32\kerberos.dll
\windows\system32\kernel32.dll
\windows\system32\Iinkinfo.dll

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

\windows\system32\lmhsvc.dll
\windows\system32\localspl.dll
\windows\system32\lsasrv.dll
\windows\system32\lsass.exe
\windows\system32\mfc42.dll
\windows\system32\midimap.dll
\windows\system32\mnmdd.dll
\windows\system32\mpr.dll
\windows\system32\mprapi.dll
\windows\system32\msacm32.dll
\windows\system32\msasnI.dll
\windows\system32\msctf.dll
\windows\system32\msgina.dll
\windows\system32\msi.dll
\windows\system32\msidle.dll
\windows\system32\msimg32.dll
\windows\system32\msisip.dll
\windows\system32\mspatcha.dll
\windows\system32\msprivs.dll
\windows\system32\mstask.dll
\windows\system32\mstlsapi.dll
\windows\system32\msutb.dll
\windows\system32\msvl_0.dll
\windows\system32\msvcp60.dll
\windows\system32\msvcrt.dll
\windows\system32\mswsock.dll
\windows\system32\msxml3.dll
\windows\system32\mtxclu.dll
\windows\system32\ncobjapi.dll
\windows\system32\nddeapi.dll
\windows\system32\netapi32.dll
\windows\system32\netcfgx.dll
\windows\system32\netlogon.dll
\windows\system32\netman.dll
\windows\system32\netmsg.dll
\windows\system32\netrap.dll
\windows\system32\netshell.dll
\windows\system32\netui0.dll
\windows\system32\netuil.dll
\windows\system32\ntdll.dll
\windows\system32\ntdsapi.dll
\windows\system32\ntlanman.dll
\windows\system32\ntmarta.dll
\windows\system32\ntoskrnl.exe
\windows\system32\ntshrui.dll
\windows\system32\odbc32.dll
\windows\system32\odbcint.dll

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

\windows\system32\ole32.dll
\windows\system32\oleacc.dll
\windows\system32\oleaut32.dll
\windows\system32\pautoenr.dll
\windows\system32\pjlmon.dll
\windows\system32\powrprof.dll
\windows\system32\profmap.dll
\windows\system32\psapi.dll
\windows\system32\psbase.dll
\windows\system32\pstorsvc.dll
\windows\system32\rasadlilp.dll
\windows\system32\rasapi32.dll
\windows\system32\raschap.dll
\windows\system32\rasdlg.dll
\windows\system32\rasman.dll
\windows\system32\rastls.dll
\windows\system32\regapi.dll
\windows\system32\regsvc.dll
\windows\system32Vresutils.dll
\windows\system32\riched20.dll
\windows\system32\rpcrt4.dll
\windows\system32\rpcss.dll
\windows\system32\rsaenh.dll
\windows\system32\rtutils.dll
\windows\system32\rundll32.exe
\windows\system32\samlib. dll
\windows\system32\samsrv.dll
\windows\system32\scecli.dll
\windows\system32\scesrv.dll
\windows\system32\schannel.dll
\windows\system32\schedsvc.dll
\windows\system32\seclogon.dll
\windows\system32\secur32.dll
\windows\system32\sens.dll
\windows\system32\services.exe
\windows\system32\setupapi.dll
\windows\system32\sfc.exe
\windows\system32\sfc_os.dll
\windows\system32\sfcfiles.dll
\windows\system32\shdoclc.dll
\windows\system32\shdocvw. dll
\windows\system32\shell32.dll
\windows\system32\shfolder.dll
\windows\system32\shimeng.dll
\windows\system32\shlwapi.dll
\windows\system32\shsvcs.dll
\windows\system32\smss.exe

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

\windows\system32\spoolss.dll
\windows\system32\spoolsv.exe
\windows\system32\srsvc.dll
\windows\system32\srvsvc.dll
\windows\system32\ssdpapi.dll
\windows\system32\ssdpsrv.dll
\windows\system32\stobject.dll
\windows\system32\svchost.exe
\windows\system32\sxs.dll
\windows\system32\tapi32.dll
\windows\system32\tcpmon.dll
\windows\system32\termsrv.dll
\windows\system32\themeui.dll
\windows\system32\trkwks.dll
\windows\system32\twext.dll
\windows\system32\umpnpmgr.dll
\windows\system32\upnp.dll
\windows\system32\urlmon.dll
\windows\system32\usbmon.dll
\windows\system32\user32.dll
\windows\system32\userenv.dll
\windows\system32\userinit.exe
\windows\system32\uxtheme.dll
\windows\system32\version.dll
\windows\system32\vga.dll
\windows\system32\vga256.dll
\windows\system32\vga64k.dll
\windows\system32\vssapi.dll
\windows\system32\w32time.dll
\windows\system32\watchdog.sys
\windows\system32\wbem\esscli.dll
\windows\system32\wbem\fastprox.dll
\windows\system32\wbem\ncprov.dll
\windows\system32\wbem\repdrvfs.dll
\windows\system32\wbem\wbemcomn.dll
\windows\system32\wbem\wbemcons.dll
\windows\system32wbem\wbemcore.dll
\windows\system32\wbem\wbemess.dll
\windows\system32\wbem\wbemprox.dll
\windows\system32\wbem\wbemsvc.dll
\windows\system32\wbem\wmiprvsd.dll
\windows\system32\wbem\wmisvc.dll
\windows\system32\wbem\wmiutils.dll
\windows\system32\wdigest.dll
\windows\system32\webcheck.dll
\windows\system32\webclnt.dll
\windows\system32\win32k.sys

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

\windows\system32\wm32spl.dll
\windows\system32\winhttp.dll
\windows\system32\wminet.dll
\windows\system32\winlogon.exe
\windows\system32\winmm.dll
\windows\system32\winrnr.dll
\windows\system32\winscard.dll
\windows\system32\winspool.exe
\windows\system32\winsrv.dll
\windows\system32\winsta.dll
\windows\system32\wintrust.dll
\windows\system32\wkssvc.dll
\windows\system32\wldap32. dll
\windows\system32\wlnotify.dll
\windows\system32\wmi.dll
\windows\system32\ws2_32.dll
\windows\system32\ws2help.dll
\windows\system32\wscsvc.dll
\windows\system32\wshext.dll
\windows\system32\wshnetbs.dll
\windows\system32\wshtcpip.dll
\windows\system32\wsock32.dll
\windows\system32\wtsapi32.dll
\windows\system32\wuauclt.exe
\windows\system32\wuaueng.dll
\windows\system32\wuauserv.dll
\windows\system32\wups.dll
\windows\system32\wzcsapi.dll
\windows\system32\wzcsvc.dll
\windows\system32\xpob2res.dll
\windows\system32\xpsp2res.dll
\ntldr
\ntdetect.com

Перечень ключей реестра ОС Windows, подлежащих контролю целостности:

HKLM\SYSTEM\CurrentControlSet\Control
HKLM\SYSTEM\CurrentControlSet\Services
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Лист регистрации изменений									
Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий сопроводительного докум. и дата	Подпись	Дата
Изм.	измененных	замененных	новых	аннулированных					

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения