МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Карачаево-Черкесский государственный университет имени У.Д. Алиева»
(КЧГУ)

Утверждаю

И.о. ректора КЧГУ

_____ Т.А. Узденов

«_03_» _06_ 2025 г.

ПОЛОЖЕНИЕ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

СОДЕРЖАНИЕ

Термины и определения

В настоящем Положении используются следующие термины и определения:

Анализ уязвимостей – мероприятия по выявлению, идентификации и оценке уязвимостей информационной системы в интересах определения возможности реализации угроз безопасности информации и способов предотвращения ущерба.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе).

Безопасность информации (данных) – состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

Доступность – состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационные ресурсы – совокупность данных, организованных для эффективного получения достоверной информации; документы и массивы документов в информационных системах.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Идентификация – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

Инцидент информационной безопасности – непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).

Компонент информационной системы – часть информационной системы, включающая некоторую совокупность информации и обеспечивающих ее обработку отдельных информационных технологий и технических средств.

Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также технических или иных средств.

Конфиденциальность – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Многофакторная аутентификация – аутентификация с использованием двух (двухфакторная) или более различных факторов аутентификации.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Объект доступа – единица информационного ресурса информационной системы (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) и хранимая в информационных системах в электронном виде.

Привилегированные пользователи – пользователи, наделенные наивысшими привилегиями в информационных системах (администраторы).

Роль – предопределенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и информационной системой.

Событие безопасности – идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

Субъект доступа – пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

Техническое средство – аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или прием информации в информационной системе.

Удаленный доступ – процесс получения доступа (через внешнюю сеть) к объектам доступа информационной системы из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединенным физически или логически с информационной системой, к которой он получает доступ.

Угроза – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Управление доступом – ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа.

Уязвимость – недостаток (слабость) информационной системы, который (которая) создает потенциальные или реально существующие условия для реализации или проявления угроз безопасности информации.

Целостность – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Обозначения и сокращения

АРМ	–	Автоматизированное рабочее место
АВПО	–	Антивирусное программное обеспечение
БД	–	База данных
ВИ	–	Виртуальная инфраструктура
ИБ	–	Информационная безопасность
ИР	–	Информационные ресурсы
ИС	–	Информационная система
КЗ	–	Контролируемая зона
МНИ	–	Машинные носители информации
МЭ	–	Межсетевые экраны
НСД	–	Несанкционированный доступ
ОС	–	Операционная система
ПАК	–	Программно-аппаратный комплекс
ПДн	–	Персональные данные
ПО	–	Программное обеспечение
ПОИБ	–	Подсистема обеспечения информационной безопасности
СВТ	–	Средства вычислительной техники
СЗИ	–	Средства защиты информации
СКЗИ	–	Средства криптографической защиты информации
СОВ	–	Система обнаружения вторжений
СУБД	–	Система управления базами данных
ТС	–	Технические средства
ФСБ России	–	Федеральная служба безопасности Российской Федерации
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю Российской Федерации

1. Назначение

Настоящий документ (далее – Положение) регламентирует порядок реализации мер, направленных на обеспечение информационной безопасности информационных систем (далее – ИС) федерального государственного бюджетного образовательного учреждения высшего образования «Карачаево-Черкесский Государственный Университет имени У.Д. Алиева» (далее - Учреждение).

2. Общие положения

2.1 Область применения

Требования настоящего Положения распространяются на всех сотрудников и все структурные подразделения Учреждения, задействованных в процессах обеспечения информационной безопасности, администрирования и мониторинга ИС, а также на всех сотрудников Учреждения, допущенных к конфиденциальной информации (в том числе персональным данным), обрабатываемой в ИС Учреждения.

При делегировании функций по обеспечению информационной безопасности, администрированию и мониторингу ИС Учреждения уполномоченному юридическому лицу на основании соответствующих договорных обязательств, требования настоящего Положения также распространяются на всех работников и все структурные подразделения уполномоченного юридического лица, включая обособленные подразделения, прямо или косвенно задействованные в процессах обеспечения информационной безопасности, администрирования и мониторинга ИС Учреждения.

Действие настоящего положения распространяется на всех сотрудников Учреждения. Сотрудники должны быть под роспись ознакомлены с требованиями настоящего Положения.

Контроль за исполнением настоящего Положения возлагается на Администратора информационной безопасности.

2.2 Источники разработки

Настоящее Положение разработано в соответствии с требованиями следующих нормативных правовых и методических документов, а также национальных стандартов Российской Федерации:

– Постановление Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Приказ ФСТЭК России от 13 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказ ФСБ России от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

3. Организация защиты информации, обрабатываемой в ИС Учреждения

3.1 Общие положения

В ИС Учреждения объектами защиты являются: информация, в том числе персональные данные, обрабатываемые в ИС Учреждения, технические средства (в том числе средства вычислительной техники, машинные носители информации (далее – МНИ), средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и

речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

Защита информации (в том числе персональных данных), обрабатываемой в ИС Учреждения, является составной частью работ по созданию и эксплуатации ИС Учреждения и обеспечивается на всех стадиях (этапах) их жизненного цикла: в ходе создания, в ходе внедрения, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации, в рамках подсистемы обеспечения информационной безопасности (далее – ПОИБ) ИС Учреждения.

Организационные и технические меры защиты информации, реализуемые в рамках ПОИБ ИС Учреждения, направлены на исключение:

– неправомерного доступа, копирования, предоставления или распространения информации, в том числе персональных данных, (обеспечение конфиденциальности информации);

– неправомерного уничтожения или модифицирования информации, в том числе персональных данных, (обеспечение целостности информации);

– неправомерного блокирования информации, в том числе персональных данных (обеспечение доступности информации).

Особенности контроля безопасности информации могут регулироваться дополнительными инструкциями и регламентами.

Для обеспечения защиты информации, обрабатываемой в ИС Учреждения, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации.

3.2 Назначение ответственных лиц и их основные функции

Для обеспечения организации обработки конфиденциальной информации (в том числе персональных данных) в Учреждении приказом руководителя

назначается лицо, ответственное за организацию обработки конфиденциальной информации (или персональных данных).

В основные функции ответственного за организацию обработки конфиденциальной информации (или персональных данных) входит:

– внутренний контроль за соблюдением Учреждением и его работниками законодательства Российской Федерации о защите информации и персональных данных;

– доведение до работников Учреждением положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных и конфиденциальной информации, требований к защите информации (в том числе персональных данных);

– организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществления контроля за приемом и обработкой таких обращений и запросов.

Для обеспечения защиты информации, обрабатываемой в Учреждении, приказом руководителя Учреждения назначается работник, ответственный за обеспечение безопасности информационных систем – администратор информационной безопасности ИС.

Обеспечение безопасности информации при ее обработке в Учреждении может быть частично или полностью передано уполномоченному юридическому лицу на основании соответствующих договорных обязательств.

Квалификация администратора информационной безопасности должна позволять:

– использовать стандартные возможности применяемых в составе ИС средств вычислительной техники, общего и специального программного обеспечения;

– производить внедрение, настройку и сопровождение средств защиты информации, входящих в состав ПОИБ;

– определять источник сбоев функционирования и отказа средств защиты информации, входящих в состав ПОИБ;

– восстанавливать работоспособность средств защиты информации, входящих в состав ПОИБ, после сбоя или отказа;

– проводить регламентные работы и техническое обслуживание средств защиты информации, входящих в состав ПОИБ;

– обеспечивать исполнение требований организационно-распорядительной документации в области защиты информации в рамках организационных и технических мер.

Приказом руководителя Учреждения утверждается перечень работников, доступ которых к информации, обрабатываемой в ИС, необходим для выполнения ими служебных (трудовых) обязанностей.

Также приказом руководителя Учреждения, в Учреждении должны быть назначены следующие ответственные лица:

– лица, ответственные за планирование и контроль мероприятий по защите информации в ИС Учреждения;

– лица, ответственные за выявление инцидентов и реагирование на них;

– ответственный за обезличивание персональных данных;

– ответственный за техническое обслуживание информационных систем (далее – Администратор информационных систем);

– ответственный пользователь средств криптографической защиты информации (далее – СКЗИ).

В основные функции лиц, ответственных за планирование и контроль мероприятий по защите информации входят:

– разработка и актуализация плана мероприятий по защите информации, обрабатываемой ИС Учреждения;

– определение порядка контроля выполнение мероприятий по обеспечению защиты информации, обрабатываемой в ИС Учреждения, предусмотренных утвержденным планом;

В основные функции лиц, ответственных за выявление инцидентов и реагирование на них входят:

– обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

– планирование и принятие мер по устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– планирование и принятие мер по предотвращению повторного возникновения инцидентов.

В основные функции ответственного за обезличивание персональных данных входят функции по обезличиванию персональных данных, в случаях, когда такое действие требуется.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

В основные функции Администратора ИС входит:

– работы по настройке, обслуживанию и устранению технических неполадок программно-технических средств из состава ИС Учреждения, за исключением средств защиты информации.

– работы по резервированию информации, обрабатываемой в ИС Учреждения, а также резервированию программных средств.

В основные функции ответственного пользователя СКЗИ входит:

– поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним;

– учет лиц, допущенных к работе с СКЗИ;

– безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов;

– проверка готовности криптосредств к использованию с составлением заключений о возможности их эксплуатации;

– контроль исполнения требований нормативных актов в области защиты информации с помощью СКЗИ;

– контроль исполнения требований эксплуатационно-технической документации СКЗИ.

3.3 Обеспечение неизменности среды функционирования

Обеспечение неизменности среды функционирования направлено на минимизацию возможностей внедрения в ИС Учреждения уязвимостей, использование которых потенциальными нарушителями безопасности информации может привести к нарушению установленных для обрабатываемой информации характеристик безопасности, а также нарушению штатного функционирования ИС Учреждения.

3.3.1. Контроль состава программных средств

К установке в ИС Учреждения допускается только то программное обеспечение или компоненты программного обеспечения, которые перечислены в техническом паспорте ИС или в сформированных списках разрешенного к использованию в ИС ПО.

Установка ПО, не входящего в перечень разрешенного производится только по согласованию с администратором информационной безопасности путем заполнения заявки (форма заявки установлена в Приложении № 1).

Настройка параметров установки и выбор конфигурации компонентов программного обеспечения (при их наличии) производится в соответствии с

документацией на программное обеспечение и организационно-распорядительной документацией по защите информации.

ПО, не входящее в состав данного Положения может быть также установлено на АРМ пользователей Администратором информационных систем по согласованию или заданию специалиста Администратора информационной безопасности в случаях:

- устранения уязвимостей в ПО;
- плановой замены используемого пользователями ПО;
- внедрения новых информационных технологий.

Для установки ПО, пользователь готовит заявку на установку ПО на имя Администратора информационной безопасности. Администратор информационной безопасности анализирует заявку и в случае положительного решения согласует ее и передает на исполнение Администратору информационных систем. После установки (удаления, замены) программного обеспечения, администратор информационных систем или работник, подчиняющийся Администратору, проводивший установку ПО вносит сведения об установленном ПО в журнал регистрации дополнений ПО (далее – Журнал) (форма Журнала установлена в Приложении № 2).

Перед установкой нового ПО необходимо провести полный антивирусный контроль дистрибутива, с которого производится установка ПО.

Отладочные и экспериментальные работы (апробирование программ) проводится с применением тестовой (условной) информации в свободное от обработки конфиденциальной информации время.

В случае обнаружения не декларированных (не описанных в документации) возможностей программного средства, исполнители (пользователи или операторы) немедленно докладывают начальнику своего подразделения. Дальнейшее использование программного средства до получения специальных указаний прекращается.

Исполнители заявки, в части их касающейся, обязаны знать документацию на программное средство и уметь правильно его эксплуатировать. Ознакомление

и обучение пользователей работе с ПО в пределах выполняемых функций проводит Администратор информационной безопасности или Администратор информационных систем.

Настройка прав доступа к устанавливаемому ПО при использовании в составе ИС средств защиты выполняется Администратором информационной безопасности в соответствии с установленной политикой безопасности.

Установка компонентов программного обеспечения осуществляется только от имени учетных записей привилегированных пользователей ИС Учреждения.

Контроль за установкой программного обеспечения, а также периодический контроль установленного в ИС Учреждения программного обеспечения на предмет его соответствия перечню программного обеспечения, приведенного в техническом паспорте (или списках разрешенного к использованию ПО), осуществляется администратором информационной безопасности в рамках проведения контроля защищенности в соответствии с пунктом 7 настоящего Положения.

В случае выявления несоответствия программного обеспечения перечню программного обеспечения, приведенному в техническом паспорте (или списках разрешенного ПО), данный факт рассматривается как инцидент информационной безопасности и Администратор информационной безопасности должен действовать в соответствии с пунктом 5 настоящего Положения. Несанкционированно установленное ПО незамедлительно удаляется.

Обновление прикладного и системного программного обеспечения технических средств ИС Учреждения производится Администратором информационных систем по мере выпуска производителями необходимых обновлений. Обновление программного обеспечения средств защиты информации, используемых в ИС Учреждения производится Администратором информационной безопасности.

Допускается устанавливать только те обновления, которые были получены из доверенных источников.

Перед установкой обновлений соответствующие дистрибутивы должны быть переданы администратору информационной безопасности для проведения следующих проверок:

– поиск известных уязвимостей с использованием в том числе базы данных уязвимостей ФСТЭК России (БДУ ФСТЭК);

– поиск признаков вредоносного программного кода с использованием средства антивирусной защиты.

Контроль установки обновлений программного обеспечения осуществляется администратором информационной безопасности с периодичностью не реже раза в квартал.

При контроле установки обновлений проверяется, в частности, актуальность используемых баз данных вирусных сигнатур средств антивирусной защиты, баз решающих правил средств межсетевого экранирования и обнаружения вторжений и баз данных уязвимостей средств анализа защищенности, иных баз средств защиты информации.

Для программного обеспечения ИС Учреждения, включая программное обеспечение средств защиты информации, должна быть предусмотрена возможность восстановления при возникновении нештатных ситуаций.

Возможность восстановления программного обеспечения предусматривает:

– восстановление системного и прикладного программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения;

– восстановление программного обеспечения базовой системы ввода-вывода с помощью штатных средств (из резервной копии) либо с помощью специального аппаратного программатора;

– восстановление и проверку работоспособности подсистемы обеспечения информационной безопасности или ее отдельных компонентов;

– возврат ИС Учреждения в начальное состояние (до возникновения нештатной ситуации), обеспечивающий их штатное функционирование, или

восстановление отдельных функциональных возможностей, позволяющих решать задачи по обработке информации в необходимом объеме.

Для восстановления программного обеспечения должны использоваться резервирование программного обеспечения, а также конфигураций программного обеспечения и средств защиты информации в соответствии с разделом 11 настоящего Положения.

3.3.2. Контроль состава технических средств

К использованию в ИС Учреждения допускаются только те технические средства или компоненты технических средств, которые перечислены в техническом паспорте ИС Учреждения.

В случае необходимости расширения/изменения перечня используемых технических средств, соответствующее решение принимается в соответствии с порядком управления конфигурацией, приведенным в пункте 6 настоящего Положения.

В случае выявления несоответствия состава технических средств, используемых в составе ИС Учреждения и подсистемы обеспечения информационной безопасности ИС Учреждения, перечню технических средств, приведенному в техническом паспорте, Администратор информационной безопасности должен действовать в соответствии с пунктом 5 настоящего Положения.

3.3.3. Контроль функционирования средств защиты информации

Контроль работоспособности, параметров настройки и правильности функционирования средств защиты информации включает в себя следующие работы:

– контроль работоспособности (неотключения) средств защиты информации;

– проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) средств защиты информации;

– контроль соответствия настроек средств защиты информации

параметрам настройки, приведенным в проектной и эксплуатационной документации на подсистему обеспечения информационной безопасности или рекомендациями производителя на данные средства.

– восстановление работоспособности (правильности функционирования) и параметров настройки средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

Контроль работоспособности, параметров настройки и правильности функционирования средств защиты информации осуществляется Администратором информационной безопасности.

Контроль осуществления разграничения доступа в ИС Учреждения включает в себя следующие работы:

– контроль правил генерации и смены паролей пользователей;

– контроль заведения и удаления учетных записей пользователей;

– контроль реализации правил разграничения доступом;

– контроль реализации полномочий пользователей;

– контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей;

– устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступа, установлением полномочий пользователей.

Контроль осуществления разграничения доступа в ИС Учреждения осуществляется Администратором информационной безопасности.

3.4 Обеспечение регистрации и мониторинга событий безопасности

Обеспечение регистрации и мониторинга событий безопасности в ИС Учреждения направлено на постоянную фиксацию и контроль проявлений состояний ИС Учреждения и ее подсистемы обеспечения информационной безопасности, указывающих на возможность нарушения конфиденциальности,

целостности или доступности информации, подлежащей защите, доступности компонентов ИС Учреждения, нарушения процедур, установленных настоящим Положением и (или) иными организационно-распорядительными документами по защите информации в ИС Учреждения, а также на нарушение штатного функционирования средств защиты информации.

Регистрация событий безопасности в ИС Учреждения обеспечивается средствами защиты информации, а также встроенными возможностями ПО, используемого в ИС Учреждения.

Права на изменение/удаление файлов журналов регистрации событий системного, прикладного программного обеспечения, и средств защиты информации должны быть предоставлены только Администратору информационной безопасности, попытки изменения настроек средств защиты информации регистрируются в журналах безопасности.

Устранение сбоев при регистрации событий (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) осуществляется Администратором информационных систем в отношении журналов регистрации общесистемного ПО и Администратором информационной безопасности в отношении журналов регистрации СЗИ.

При переполнении журналов регистрации событий информационной безопасности, Администратор информационной безопасности копирует содержимое журналов на учтённый установленным образом носитель информации и очищает журнал. При необходимости увеличивается квота на размер журнала.

3.4.1. Состав событий безопасности и сроки их хранения

В ИС Учреждения подлежат регистрации следующие события безопасности:

– вход (выход), а также попытки входа субъектов доступа в операционную систему и загрузки (останова) операционной системы в составе: дата и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат

попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа;

– подключение МНИ в составе: дата и время подключения МНИ, логическое имя (номер) подключаемого машинного носителя информации;

– запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации, в составе: дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный);

– попытки доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам в составе: дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификация защищаемого файла (логическое имя, тип);

– попытки доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) и иным объектам доступа в составе: дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификация защищаемого объекта доступа (логическое имя (номер);

– попытки удаленного доступа в составе: дата и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа).

Перечень событий безопасности, подлежащих регистрации в ИС Учреждения, уточняется по результатам контроля (анализа) защищенности, но не менее чем один раз в год.

Хранение информации о зарегистрированных событиях безопасности и записей системных журналов, которые послужили основанием для регистрации события безопасности, производится в течение трех месяцев.

Объем памяти для хранения событий безопасности ИС Учреждения в течение указанного времени устанавливается Администратором информационных систем в отношении журналов регистрации событий прикладного программного обеспечения и Администратором информационной безопасности в отношении журналов регистрации событий средств защиты информации, включая системное программное обеспечение, с учетом прогнозируемой частоты возникновения подлежащих регистрации событий безопасности.

Устранение сбоев при регистрации событий (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) осуществляется администратором информационных систем в отношении журналов регистрации событий прикладного программного обеспечения и администратором информационной безопасности в отношении журналов регистрации событий средств защиты информации, включая системное программное обеспечение.

3.4.2. Мониторинг результатов регистрации событий безопасности

Мониторинг событий безопасности, подлежащих регистрации в ИС Учреждения, с целью своевременного выявления признаков инцидентов безопасности осуществляется Администратором информационной безопасности. Просмотр журналов событий осуществляется при возникновении инцидента информационной безопасности или, в случае отсутствия инцидентов, не реже одного раза в месяц.

При необходимости, для получения полной информации о событии информационной безопасности, Администратор информационной безопасности изучает также журналы ОС и (или) специализированного ПО.

В случае выявления признаков инцидентов безопасности, Администратор информационной безопасности должен действовать согласно пункту 5 настоящего Положения.

3.4.3. Методы защиты информации о событиях безопасности

В ИС Администратором ИБ должны использоваться следующие методы защиты информации о событиях безопасности:

– логическое ограничение доступа к местам хранения журналов событий.

– управление журналами событий. Доступ к управлению журналами должен быть разрешен только для привилегированных пользователей ИС.

Контроль реализации методов защиты осуществляется Администратором ИБ не реже одного раза в год.

3.5 Правила и процедуры генерирования временных меток и синхронизация системного времени в ИС

Администратор информационной безопасности для каждого узла и сегмента ИС:

– устанавливает службы протокола сетевого времени (NTP) с одними и теми же источниками (NTP-серверами).

– в отсутствии возможности установки службы протокола сетевого времени, производит синхронизацию часов и календаря узлов и сегментов ИС с погрешностью не более одной минуты ежемесячно.

3.6 Обеспечение контролируемой зоны и защита технических средств

Границы контролируемой зоны устанавливаются исходя из границ пространства (территории, здания, часть здания), в котором исключено неконтролируемое пребывание лиц, а также технических или иных средств.

Границей контролируемой зоны как минимум должен являться периметр помещений, в которых размещены ИС Учреждения и компоненты подсистемы обеспечения информационной безопасности. Граница контролируемой зоны ИС Учреждения определяется приказом руководителя Учреждения. Для ИС может быть организовано несколько контролируемых зон.

Контроль доступа к средствам вычислительной техники и средствам криптографической защиты информации в ИС Учреждения реализуется путем:

– опечатывания корпуса АРМ пользователя и серверов ИС Учреждения специальным опечатывающим материалом, сигнализирующим о нарушении целостности (попытках вскрытия);

– утверждения правил доступа к средствам вычислительной техники и средствам криптографической защиты информации в рабочее и нерабочее время, а также в нештатных ситуациях;

– утверждения перечня лиц, имеющих право доступа к средствам вычислительной техники и средствам криптографической защиты информации;

Правила доступа к средствам вычислительной техники и средствам криптографической защиты информации ИС Учреждения, являются следующими:

– в рабочее и нерабочее время доступ к средствам вычислительной техники и средствам криптографической защиты информации предоставляется только легитимным пользователям ИС Учреждения;

– в нештатных ситуациях доступ к средствам вычислительной техники и средствам криптографической защиты информации предоставляется представителям производителя (изготовителя) ИС Учреждения под контролем привилегированного пользователя ИС Учреждения.

Лица, имеющие доступ к средствам вычислительной техники и средствам криптографической защиты информации не должны передавать свои средства доступа третьим лицам.

Размещение устройств вывода (отображения) защищаемой информации должно исключать возможность несанкционированного просмотра отображаемой защищаемой информации как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны.

Потенциальные направления визуального съема информации определяются Администратором информационной безопасности. Администратор информационной безопасности контролирует расположение

устройств вывода (отображения и печати) информации и их изменение расположения пользователями.

Администратор информационной безопасности должен исключить нахождение в помещениях ИС лиц, которым не разрешен доступ к средствам вычислительной техники и защищаемой информации, оконные жалюзи помещений при работе с защищаемой информацией закрываются. При необходимости проведения в помещении ИС каких-либо работ, не связанных с обработкой информации, АРМ данной ИС блокируется, монитор выключается, документы, содержащие защищаемую информацию, убираются в сейф или запирающийся ящик стола. Персонал сторонних организаций производит работы исключительно в сопровождении работника ИС Учреждения. Проведение таких работ производится с разрешения руководителя Учреждения.

Для обеспечения защиты технических средств могут применяться следующие технические средства:

– двери, расположенные по периметру контролируемой зоны, должны быть оборудованы механическим замком;

– окна, расположенные по периметру контролируемой зоны, должны быть оснащены системами открывания с внутренней стороны;

– дополнительно могут применяться системы контроля и управления доступом, металлические решетки на окнах, охранные датчики (движения, открытия, разбития стекол и т.д.), видеонаблюдение.

Запрещается оставлять помещение незапертым в моменты отсутствия в нем лиц, допущенных в контролируемую зону.

4. Управление доступом

4.1 Методы и правила идентификации и аутентификации

Каждой пользовательской роли назначается минимально необходимый набор прав и привилегий, достаточный для выполнения соответствующих обязанностей.

Пользователи ИС Учреждения однозначно идентифицируются для всех видов доступа.

Организационное обеспечение процессов генерации, инициализации, хранения, выдачи, использования, смены, блокирования и прекращения действия паролей в ИС, за правильную реализацию настоящих правил и процедур идентификации и аутентификации субъектов доступа к объектам доступа осуществляет Администратор информационной безопасности.

В ИС Учреждения используются два типа идентификаторов и аутентификаторов:

– ученая запись для работы в прикладном и специализированном ПО;

– учетная запись в операционной системе АРМ.

В отношении использования паролей для аутентификации устанавливаются следующие требования:

– длина пароля должна составлять не менее 8 (восьми) символов;

– алфавит пароля должен составлять не менее 60 (шестидесяти) символов;

– максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки учетной записи должно составлять от 3 до 10 (трех до десяти) попыток;

– обязательная смена пароля должна производиться не более чем через 90 (девяносто) дней с момента начала его использования.

Блокировка учетной записи пользователя возможна при достижении установленного максимального количества неуспешных попыток аутентификации – на срок от 5 до 30 (пяти до тридцати минут).

Для субъектов доступа устанавливаются пароли следующих типов:

– администраторский;

– операторский;

– пользовательский.

Администраторский пароль предназначен для реализации полного доступа к ресурсам соответствующей ИС с правами изменения всех параметров

конфигурации, предоставления субъектам доступа прав административного или пользовательского доступа.

Пользовательский пароль предназначен для доступа к ресурсам соответствующей ИС Учреждения с правами, минимально необходимыми для выполнения прикладных задач, в рамках функциональных обязанностей субъекта доступа.

Для генерации «стойких» паролей могут применяться специальные программные средства (системы генерации паролей). Система генерации паролей должна исключать возможность ознакомления других субъектов доступа с генерируемыми значениями паролей.

Пароль не должен включать в себя легко вычисляемые сочетания символов, например:

– имя или фамилия пользователя;

– день рождения и другие памятные даты;

– другие данные, которые могут быть подобраны путем анализа информации о пользователе;

– последовательности подряд идущих символов клавиатуры (например, «1234567» или «qwerty» и т. п.);

– повторяющийся символ, либо повторяющаяся комбинация из нескольких символов (например, «111111» или «w2w2w2» и т.п.);

– использование одной цифры до или после слова (например, «Password1»);

– замена букв на схожие по написанию цифры (например, «pa55w0rd»).

В ИС Учреждения исключено отображение действительного значения паролей пользователей и количества вводимых символов. Пользователю ИС запрещается ввод аутентификационной информации в случае, если существует возможность наблюдения за вводом со стороны посетителей или посторонних лиц.

Покидая рабочее место, сотрудник должен заблокировать экран. Обеспечивается блокирование сеанса доступа работника после времени

бездействия (неактивности) пользователя – до 5 минут. Для возобновления сеанса работы пользователь вводит пароль, соответствующий его учётной записи. СЗИ от НСД настраивается таким образом, чтобы запретить пользователю ИС любые действия до прохождения процедур идентификации и аутентификации. Действия, проводимые до процедур идентификации и аутентификации разрешаются исключительно Администратору информационной безопасности в целях восстановления работоспособности ИС.

Запрещается повторно использовать идентификатор пользователя в течение не менее одного года.

Администратор ИБ обязан блокировать или инициировать блокировку идентификаторов пользователей через период времени неиспользования более 90 дней.

Для всех технических и программных средств ИС Учреждения и подсистемы обеспечения информационной безопасности запрещается использование идентификационной и аутентификационной информации, заданной по умолчанию производителями (поставщиками).

При необходимости восстановления идентификационной и аутентификационной информации, заданной по умолчанию, (например, в случае утери действующей идентификационной и аутентификационной информации) смена указанной информации должна быть произведена незамедлительно.

Пользователям запрещается разглашать идентификационную и аутентификационную информацию. Внеплановая смена идентификационной и аутентификационной информации пользователя, блокирование или удаление учетной записи пользователя ИС, в случае прекращения его полномочий (отпуск, увольнение и прочее), должна производиться Администратором информационной безопасности незамедлительно после окончания последнего сеанса работы данного пользователя в ИС.

В случае нештатных ситуаций право доступа к парольной информации учетной записи имеют администратор информационной безопасности, а также лица их замещающие.

В случае компрометации идентификационной и аутентификационной информации пользователя ИС должны незамедлительно быть предприняты меры по ее замене и выявлению последствий компрометации.

4.2 Регистрация учетных записей пользователей

Процедура регистрации (создания учетной записи) пользователя и предоставления (или изменения) ему прав доступа к ИС инициируется приказом руководителя Учреждения о допуске пользователей к работе в ИС, заявкой руководителя структурного подразделения. (форма заявки установлена в Приложении 3).

В заявке указывается:

– содержание запрашиваемых изменений (регистрация нового пользователя ИС, удаление учетной записи пользователя, расширение или исключение полномочий и прав доступа к ИС ранее зарегистрированного пользователя);

– должность (с полным наименованием структурного подразделения, организации, если внешний пользователь), фамилия, имя и отчество работника;

– имя пользователя (учетной записи) данного работника;

– полномочия, которые необходимо добавить (путем указания решаемых пользователем задач в ИС) или исключить пользователю.

Заявку визирует вышестоящий руководитель, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного пользователя к необходимым для решения им указанных задач в ИС.

На основании заявки (задания) Администратор информационной безопасности в соответствии с документацией на средства защиты информации производит необходимые операции по созданию (регистрации), изменению, блокированию, удалению учетной записи пользователя, присвоению ему начального значения пароля и заявленных прав доступа к ИС, включению его в соответствующие группы пользователей и иные необходимые действия.

По окончании внесения изменений в списки пользователей в заявке проставляется отметка о выполнении задания.

Работнику, зарегистрированному в качестве нового пользователя ИС, под роспись сообщается имя соответствующего ему пользователя, при необходимости выдается персональный электронный идентификатор и начальное значение пароля, которое он обязан сменить при первом же входе в ИС.

Исполненная заявка хранится совместно с документацией на ИС у лица, ответственного за организацию обработки конфиденциальной информации (или персональных данных).

4.3 Правила и процедуры определения действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации

Действия пользователей до прохождения ими процедуры идентификации и аутентификации в ИС запрещены.

Загрузка АРМ ИС предусмотрена с жёсткого диска, данный вариант загрузки настраивается в BIOS материнской платы АРМ. Доступ к настройкам BIOS материнской платы АРМ в случае необходимости может защищаться средствами доверенной загрузки, сертифицированных по требованиям ФСТЭК России. Средство доверенной загрузки может быть программным, аппаратным, программно-аппаратным.

4.4 Методы и правила разграничения доступа

Для разграничения прав доступа к ресурсам ИС могут использоваться следующие методы разграничения доступа:

– дискреционный (управление доступом для индивидуального субъекта доступа);

– ролевой (управление доступом по группам субъектов доступа);

– мандатный (сопоставление классификационных меток каждого субъекта доступа и каждого объекта доступа).

Методы разграничения доступа в ИС определяются на этапе проектирования ИС (или ПОИБ ИС) или в процессе функционирования ИС Администратором информационной безопасности. Типы доступа определяют операции по чтению, записи, удалению и выполнению, разрешенные к выполнению пользователем или запускаемому от его имени процессу при доступе к объектам доступа.

Правила разграничения доступа, настроенные в ИС Учреждения, обеспечивают:

– управление доступом при входе в операционную систему;

– управление доступом к портам ввода-вывода;

– управление доступом к объектам, создаваемым программным обеспечением, в том числе к объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным программным обеспечением.

Администратор информационной безопасности осуществляет управление учетными записями пользователей путем их заведения, активации, блокирования и уничтожения. Управление учетными записями осуществляется в соответствии с разрешительной системой доступа (перечнем наличия прав доступа субъектов доступа к информационным ресурсам).

Сетевое оборудование должно быть сконфигурировано таким образом, чтобы защищаемая информация, циркулировала по каналам связи в соответствии с разработанными правилами разграничения доступа.

Набор прав и полномочий для различных категорий пользователей и администратора информационной безопасности должен различаться.

Назначение прав и полномочий должно производиться по запросу, с согласования Администратора информационной безопасности.

В ИС может быть создана временная учетная запись, которая заводится на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для произведения настройки, тестирования информационной системы, для организации гостевого доступа. После выполнения задач,

временная учетная запись должна быть заблокирована или удалена Администратором информационной безопасности.

В ИС Учреждения осуществляется автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования, автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования – более 45 дней.

Для доступа к наиболее критичным процессам обработки, хранения, передачи и защиты информации в ИС Учреждения могут использоваться дополнительные индивидуальные электронные идентификаторы (eToken, iButton, смарт-карты и иные идентификаторы).

Дополнительные идентификаторы выдаются администратором информационной безопасности ИС Учреждения, при этом:

– полномочные субъекты доступа получают дополнительные идентификаторы под подпись;

– администратор информационной безопасности Учреждения ведет учет выданных дополнительных идентификаторов и проводит инструктаж работников по выполнению правил их эксплуатации (использования).

Субъекты доступа, получившие в пользование дополнительные идентификаторы, лично обеспечивают надежное круглосуточное безопасное хранение и использование идентификаторов. Оставление идентификатора без присмотра запрещается.

В случае утери дополнительного идентификатора субъекты доступа немедленно ставят об этом в известность администратора информационной безопасности Учреждения и своего непосредственного руководителя. Администратор информационной безопасности организует немедленную блокировку утерянных ключей.

5. Управление конфигурацией

5.1 Общие требования к управлению конфигурацией

В рамках управления конфигурацией ИС Учреждения в ходе эксплуатации должны осуществляться:

– управление изменениями конфигурации ИС Учреждения и подсистемы обеспечения информационной безопасности;

– анализ потенциального воздействия планируемых изменений в конфигурации ИС Учреждения и подсистемы обеспечения информационной безопасности на состояние защищенности ИС Учреждения и согласование изменений в конфигурации с Администратором информационной безопасности;

– документирование информации об изменениях в конфигурации ИС Учреждения и подсистемы обеспечения информационной безопасности.

Правом на внесение изменений в конфигурацию ИС Учреждения и подсистемы обеспечения информационной безопасности обладают привилегированные пользователи ИС Учреждения с учетом разграничения их полномочий согласно настоящему Положению.

5.2 Инициация внесения изменений в конфигурацию

Внесение изменений в конфигурацию может быть инициировано в следующих случаях:

– в рамках доработки (модернизации) ИС Учреждения или его компонентов;

– в рамках устранения нештатных ситуаций, требующих замены оборудования, его компонентов, системного программного обеспечения или средств защиты информации.

Все запросы на изменение конфигурации ИС Учреждения или ее отдельных компонентов должны быть переданы на рассмотрение Администратору информационной безопасности.

5.3 Оценка потенциального воздействия изменений

Оценка потенциального воздействия изменений должна быть выполнена для всех субъектов изменений, а также для всех взаимосвязанных с ними информационных ресурсов и компонентов ИС Учреждения.

Оценка потенциального воздействия должна включать в себя следующие направления:

– оценка технического воздействия и совместимости;

– оценка на соответствие нормативным правовым и проектным требованиям, применимым к ИС Учреждения;

– оценка влияния на состояние защищенности ИС Учреждения;

– оценка влияния на целевые функции и процессы ИС Учреждения.

Оценка потенциального воздействия изменений, предусматривающих установку системного и прикладного программного обеспечения, а также программного обеспечения базовой системы ввода-вывода и средств защиты информации, включая пакеты обновлений (патчи), должна предусматривать передачу соответствующих дистрибутивов администратору информационной безопасности для проведения следующих проверок:

– поиск известных уязвимостей с использованием базы данных угроз безопасности ФСТЭК России;

– поиск признаков вредоносного программного кода с использованием средства антивирусной защиты.

Установка программного обеспечения, включая пакеты обновлений (патчи), содержащего известные уязвимости или вредоносный программный код, запрещена.

Все изменения до внедрения должны быть в обязательном порядке согласованы администратором информационной безопасности.

5.4 Внесение изменений в конфигурацию

Внесение изменений в конфигурацию ИС Учреждения производится привилегированными пользователями ИС Учреждения с учетом разграничения

их полномочий согласно настоящему Положению с привлечением по необходимости представителей производителя (изготовителя) ИС Учреждения.

Информация о произведенных изменениях вносится в Журнал регистрации изменений в конфигурации ИС (форма журнала установлена в Приложении № 5) и включает в себя следующие данные:

– краткое описание конфигурационного изменения;

– цель производимого конфигурационного изменения;

– наименование компонента ИС Учреждения, в конфигурации которого произведено изменение;

– дата и время произведенного конфигурационного изменения;

– подпись ответственного должностного лица.

В случае, если изменение конфигурации ИС Учреждения влечет необходимость актуализации информации, приведенной в техническом паспорте, его актуализация производится лицом, внесшим изменение в конфигурацию в срок, не превышающий 3 дней с момента внесения изменений в конфигурацию.

Актуализированная версия технического паспорта передается администратору информационной безопасности для учета.

5.5 Порядок технического обслуживания и ремонта технических средств ИС

Техническое обслуживание и ремонтные работы на технических средствах ИС должны осуществляться только уполномоченными работниками, назначенными ответственными за их обслуживание (сопровождение). Их вызов осуществляется работниками подразделения, эксплуатирующего конкретную ИС, при возникновении нештатных ситуаций.

К нештатным ситуациям относятся:

- выход из строя или неустойчивое функционирование АРМ, серверов или периферийных устройств (например, дисковода, принтера);

- выход из строя системы электроснабжения ИС.

Все нештатные ситуации фиксируется Администратором информационной безопасности в Журнале учета нештатных ситуаций (форма журнала установлена в Приложении № 6).

Техническое обслуживание и регламентные работы могут проводиться в плановом порядке. В этом случае работы проводятся на основании утвержденных руководством и согласованных с Администратором информационной безопасности заявок.

Ответственность за соблюдение требований по обеспечению безопасности информации при проведении технического обслуживания и ремонтных работ возлагается на Администратора информационной безопасности.

Уполномоченные работники допускаются к ИС для разбора нештатных ситуаций при обнаружении сбоев в работе только для тестирования АРМ или серверов с использованием установленных в ИС тестовых средств.

По окончании выполнения данных работ составляется акт с указанием признаков проявления ситуации и содержанием выполненных работ по ее устранению.

При необходимости осуществления изменений аппаратной конфигурации ИС, прошедших аттестационные испытания, соответствующие работы выполняются по согласованию с организацией, проводившей аттестационные испытания ИС.

В случае, если внесенные изменения затронули статус Аттестата соответствия, Учреждением должен быть рассмотрен вопрос о проведении повторной аттестации ИС или проведении дополнительных аттестационных испытаний на соответствие требованиям безопасности информации.

При изъятии АРМ и серверов, их передача на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как Администратор информационной безопасности снимет с АРМ и серверов средства защиты информации, жесткие диски и предпримет необходимые меры для затирания защищаемой информации, которая хранилась на дисках АРМ.

Оригиналы документов, на основании которых производились изменения в составе аппаратно-программных средств ИС, и акты о внесении изменений в состав аппаратно-программных средств должны храниться вместе с оригиналами аттестационных документов ИС.

6. Действия при нештатных ситуациях

Общими требованиями ко всему персоналу ИС Учреждения с правом доступа к ресурсам ИС Учреждения, в случае возникновения нештатной ситуации является:

– при возникновении нештатных ситуаций с угрозой нарушения требований документов организационно-распорядительной документации по защите информации, в том числе настоящего Положения работник, обнаруживший нештатную ситуацию немедленно ставит в известность своего непосредственного руководителя и администратора информационной безопасности;

– администратор информационной безопасности ИС Учреждения проводит анализ ситуации;

– в случае невозможности исправить сложившееся положение дел информирует руководителя Учреждения;

– для локализации (блокирования) проявлений угроз, администратор информационной безопасности привлекает администратора информационных систем;

– по факту возникновения нештатной ситуаций и выяснению причин ее проявления в Учреждении проводится служебное расследование.

7. Действия персонала при возникновении нештатных ситуаций

7.1 Действия при стихийных бедствиях, пожарах или наводнениях

При возникновении нештатной ситуаций, работник обязан:

– оповестить других работников;

– оповестить соответствующие службы (пожарная охрана, служба спасения);

– сообщить непосредственному руководителю и администратору информационной безопасности;

– принять меры к эвакуации оборудования ИС Учреждения и устранения последствий стихийного бедствия.

7.2 Действия в случае несанкционированного доступа к оборудованию

При возникновении ситуации работник обязан:

– сообщить непосредственному руководителю и администратору информационной безопасности;

– принять меры по сохранности свидетельств взлома, несанкционированного проникновения и/или получения доступа к оборудованию ИС Учреждения;

– по прибытию администратора информационной безопасности действовать по его указаниям.

При получении сообщения по факту получения несанкционированного доступа к оборудованию ИС Учреждения администратор информационной безопасности сообщает о случившемся своему непосредственному руководителю или напрямую руководителю Учреждения, обеспечивает выполнение мер обеспечения сохранности свидетельств: взлома, несанкционированного проникновения и/или получения доступа к оборудованию ИС Учреждения до прибытия представителей правоохранительных органов.

Администратор информационной безопасности вызывает представителей органов правопорядка для принятия мер по расследованию данного происшествия.

7.3 Действия в случае сбоя в работе программного обеспечения

В случае обнаружения программного конфликта между используемыми в ИС Учреждения программными средствами работник обязан:

– сообщить непосредственному руководителю и администратору информационной безопасности;

– принять меры по недопущению распространения выявленного программного конфликта на другие средства обработки и защиты информации;

– оказывать помощь администратору информационной безопасности.

Администратор информационной безопасности совместно с соответствующими администраторами выясняют причину программного конфликта (сбоя в работе программного обеспечения). В случае, если исправить ситуацию своими силами (в том числе после консультации с разработчиками программного обеспечения) не удалось, составляется акт проверки работоспособности средств и систем ИС Учреждения, в среде функционирования которых данный конфликт был обнаружен, копия которого и сопроводительные материалы, свидетельствующие о наличии данной проблемы, направляются разработчикам программного обеспечения.

7.4 Действия в случае отключения электричества

В случае внештатного отключения электричества администратор информационной безопасности совместно с соответствующими администраторами проводят анализ на наличие потерь и (или) разрушения данных и программного обеспечения, а также проверяют работоспособность оборудования ИС Учреждения. В случае необходимости производится работы по восстановлению программного обеспечения и данных из последней резервной копии с составлением акта.

7.5 Действия в случае сбоя в работе оборудования

В случае обнаружения сбоя в работе оборудования работник обязан:

– сообщить непосредственному руководителю и администратору информационной безопасности;

– оказывать помощь администратору информационной безопасности.

По факту выявленного сбоя в работе оборудования администратор информационной безопасности совместно с администратором информационных систем принимают меры по выводу из эксплуатации дефектного оборудования, проводят анализ состояния данных и (или) установленного программного

обеспечения. А при необходимости переносят информацию, хранимую на подверженном сбоям оборудовании, на другой сервер или иное СВТ ИС Учреждения. По факту выявленного сбоя оборудования АИС ОФД составляется акт проверки, обосновывающий необходимость проведения работ по его восстановлению.

Действия в случае выхода из строя серверного и иного оборудования ИС Учреждения, администратор информационной безопасности совместно с администратором информационных систем:

– принимают меры по немедленному вводу в действие резервного оборудования;

– проводят оценку технического состояния вышедшего из строя оборудования и составляют акт проверки его работоспособности, с последующей передачей его уполномоченному лицу, ответственному за организацию ремонтно-восстановительных работ в ИС Учреждения.

В случае восстановления работоспособности вышедшего из строя оборудования силами обслуживающего персонала ИС Учреждения должны быть проведены работы по восстановлению программного обеспечения и данных из резервных копий, а также тестирование данного оборудования в условиях близких к реальным.

7.6 Действия в случае потери данных

При обнаружении потери данных администратор информационной безопасности совместно с администратором информационных систем в среде функционирования которых произошла потеря данных, проводят мероприятия по поиску и устранению причин потери данных (антивирусная проверка, проверка целостность и работоспособность программного обеспечения и оборудования). По результатам выполненных работ администратором информационной безопасности разрабатываются и направляют в адрес руководителя Учреждения предложения по устранению причин возможной потери данных в дальнейшем. Потерянные данные восстанавливаются из резервных копий с составлением акта восстановления.

7.7 Действия в случае обнаружения утечки информации

В качестве основных свидетельств, подтверждающих наличие «скрытых» каналов утечки информации с использованием программных средств должны рассматриваться:

факты установки несанкционированного программного обеспечения;

– несоответствие конфигураций сетевого оборудования требованиям к маршрутизации и фильтрации сетевого трафика;

– неправомерный доступ к неконтролируемым ресурсам сети Интернет;

– наличие на рабочих станциях и серверах информационных массивов с информацией для обработки, хранения и передачи которой данные СВТ не предназначены;

– обнаружение фактов несанкционированного применения сетевых протоколов.

В случае обнаружения фактов, подтверждающих наличие «скрытых» каналов утечки информации работнику необходимо:

– сообщить непосредственному руководителю и администратору информационной безопасности;

– действовать по указаниям администратора информационной безопасности.

Работнику, обнаружившему факт наличия «скрытого» канала утечки информации, запрещается без разрешения администратора информационной безопасности сообщать об этом кому бы то ни было.

Администратор информационной безопасности:

– сообщает об этом своему непосредственному руководителю или руководителю Учреждения;

– проводит предварительный анализ возможностей нарушителя по передаче информации с использованием «скрытого» канала утечки информации;

– докладывает результаты проведенного анализа непосредственному руководителю или руководителю Учреждения.

Руководитель Учреждения:

– принимает решение по привлечению специалистов Учреждения, необходимых для проведения детального анализа возможностей по использованию «скрытого» канала утечки информации;

– совместно с администратором информационной безопасности и привлеченными специалистами Учреждения проводит оценку возможностей нарушителя по нанесению материального и/или морального ущерба Учреждения, а также свидетельств, документально подтверждающих фактическое нарушение требований положения информационной безопасности Учреждения.

На основании результатов детальной оценки принимается один из двух вариантов принятия мер:

1 вариант – ведение наблюдения за нарушителем с целью сбора необходимых доказательств, подтверждающих виновность нарушителя с последующим принятием мер по немедленному блокированию выявленного канала утечки информации, отстранению нарушителя от работы с ресурсами ИС Учреждения и проведению служебного расследования;

2 вариант – является разновидностью 1 варианта, при этом наблюдение за нарушителем не проводиться, и сразу принимаются меры по блокированию выявленного канала утечки информации, отстранению нарушителя от работы с ресурсами ИС Учреждения и проведению служебного расследования.

7.8 Действия в случае несанкционированного доступа

По выявленному факту несанкционированного доступа необходимо:

– сообщить непосредственному руководителю и администратору информационной безопасности;

– действовать по указаниям администратора информационной безопасности;

Работнику, обнаружившему взлом системы, запрещается без разрешения администратора информационной безопасности сообщать об этом кому бы то ни было.

Администратор информационной безопасности:

– сообщает своему непосредственному руководителю или руководителю Учреждения;

– принимает меры по локализации оборудования в программно-аппаратной среде которого выявлен факт взлома;

– совместно с администратором информационных систем проводит ревизию всего программного обеспечения и контроль целостности информационных ресурсов данного средства, на предмет выявления всех свидетельств реализации атаки;

– проводит внеплановую антивирусную проверку, контроль целостности файловой системы, а также иные мероприятия, целесообразность которых определяется по выявленным «следам» взлома;

– при необходимости выполняется восстановление работоспособности системы, включая установленные в ней средства защиты информации;

– совместно с администратором информационных систем проводит анализ условий и предпосылок несанкционированного проникновения в систему.

По решению администратора информационной безопасности проводится выборочная или полная проверка применяемых в ИС Учреждения мер и средств защиты от несанкционированного доступа.

7.9 Действия в случае компрометации пароля

В случае выявления факта компрометации пароля (аутентификационной информации субъекта доступа) необходимо:

– сообщить непосредственному руководителю и администратору информационной безопасности;

– действовать по указаниям администратора безопасности.

Администратор информационной безопасности:

– совместно с администратором информационных систем принимает меры по ее блокированию;

– проводит расследование факта компрометации пароля с целью определения условий и причин ее возникновения;

– в случае отсутствия вины субъекта доступа в компрометации используемого им пароля дает разрешение на предоставление ему необходимых прав доступа в соответствии с установленным регламентом;

– в течении месяца, с момента компрометации пароля, ведет контроль попыток использования учетной записи субъекта доступа, заблокированной по факту компрометации пароля, на предмет выявления потенциального нарушителя, использующего возможность получения доступа под правами зарегистрированного пользователя;

– в случае обнаружения потенциального нарушителя, использующего ранее заблокированную учетную запись, действует в соответствии с правилами реагирования на попытку получения несанкционированного доступа к ресурсам ИС Учреждения;

– при наличии свидетельств, подтверждающих причастность субъекта доступа в компрометации используемого им пароля, докладывает обстоятельства происшествия руководителю Учреждения и действует по его указаниям.

8. Контроль и анализ защищенности

8.1 Общие требования к контролю защищенности

В рамках проведения контроля (анализа) защищенности ИС Учреждения в ходе эксплуатации должны осуществляться:

– контроль за событиями безопасности в ИС Учреждения;

– контроль (анализ) защищенности информации, содержащейся в ИС Учреждения;

– анализ и оценка функционирования подсистемы обеспечения информационной безопасности, включая выявление, анализ и устранение

недостатков в функционировании средств защиты информации;

– периодический анализ изменения угроз безопасности информации ИС Учреждения, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых актуальных угроз безопасности информации;

– документирование процедур и результатов контроля (анализа) защищенности;

– принятие решения по результатам контроля (анализа) защищенности о доработке (модернизации) подсистемы обеспечения информационной безопасности, повторной аттестации или проведении дополнительных аттестационных испытаний.

8.2 Организация контроля защищенности

Контроль защищенности производится администратором информационной безопасности с привлечением при необходимости иных сотрудников, обладающих компетенциями в области обеспечения информационной безопасности.

Контроль защищенности подразделяется на периодический и внеплановый.

Периодический контроль защищенности производится в соответствии с планами проведения контроля защищенности, формируемыми администратором информационной безопасности ежегодно, с периодичностью не реже одного раза в квартал.

Периодический контроль защищенности должен включать все проверки, входящие в перечень, приведенный в пункте 7.3 настоящего Положения.

Внеплановый контроль защищенности производится в следующих случаях:

– проверка устранения замечаний, выявленных в ходе предыдущего контроля защищенности;

– проверка состояния защищенности при выявлении инцидентов

информационной безопасности (по завершению процессов, предусмотренных пунктом 5 настоящего Положения);

– проверка состояния защищенности при внесении изменений в конфигурацию в соответствии с пунктом 6 настоящего Положения.

В рамках внепланового контроля защищенности допускаются выборочные проверки из перечня, приведенного в пункте 7.3 настоящего Положения.

Результаты проведения контроля защищенности фиксируются в Журнале учета мероприятий по контролю защищенности (форма журнала установлена в Приложении № 7).

Периодический анализ изменения угроз безопасности информации ИС Учреждения, возникающих в ходе ее эксплуатации, инициируется по решению руководителя Учреждения.

8.3 Порядок проведения контроля защищенности

При выполнении контроля защищенности должны выполняться следующие мероприятия:

– проверка наличия действующих сертификатов на средства защиты информации, используемые в составе подсистемы обеспечения информационной безопасности ИС Учреждения;

– проверка корректности настроек и функционирования средств защиты информации, используемых в составе подсистемы обеспечения информационной безопасности ИС Учреждения;

– анализ уязвимостей ИС Учреждения;

– проверка фактического выполнения организационных мер защиты информации;

– проверка неизменности программно-аппаратной инфраструктуры ИС Учреждения и их соответствие техническому паспорту.

По результатам проведения контроля защищенности выявленные несоответствия и (или) замечания заносятся в Журнал учета мероприятий по контролю защищенности.

При наличии в Журнале учета мероприятий по контролю защищенности выявленных замечаний по результатам проведения контроля защищенности администратором информационной безопасности проводятся мероприятия по устранению выявленных замечаний в соответствии с приведенными рекомендациями.

После устранения замечаний проводится повторный контроль защищенности с целью подтверждения устранения выявленных замечаний.

Результаты контроля защищенности доводятся до руководителя Учреждения в случае необходимости принятия решений о доработке (модернизации) ИС Учреждения и ее подсистемы обеспечения информационной безопасности, повторной аттестации или проведении дополнительных аттестационных испытаний.

8.3.1. Проверка наличия действующих сертификатов на средства защиты информации

Проверка наличия действующих сертификатов на средства защиты информации осуществляется с использованием документации, включенной в поставку средств защиты информации, а также с использованием перечней средств защиты информации, сертифицированных в системах сертификации РОСС RU.0001.01БИ00 и РОСС RU.0001.030001, полученных из официальных ресурсов ФСТЭК России и ФСБ России посредством информационно-телекоммуникационной сети «Интернет».

В случае выявления в составе подсистемы обеспечения информационной безопасности средств защиты информации, на которые отсутствуют действующие сертификаты соответствия, данные факты включаются в Журнал учета мероприятий по контролю защищенности.

Рекомендации по устранению данного замечания могут включать в себя следующие сценарии:

– официальный запрос у производителя средства защиты информации сведений о продлении сертификата соответствия в соответствующей системе сертификации;

– внесение изменений в проектные решения подсистемы обеспечения информационной безопасности в случае, если производитель не планирует продление сертификата соответствия на соответствующее средство защиты информации, и использование компенсирующих мер защиты до приведения подсистемы обеспечения информационной безопасности в соответствие предъявляемым к ней требованиям.

8.3.2. Проверка корректности настроек и функционирования средств защиты информации

Проверка корректности настроек и функционирования средств защиты информации, используемых в составе подсистемы обеспечения информационной безопасности, осуществляется с использованием штатных интерфейсов средств защиты информации.

В рамках данной проверки производится:

– проверка соответствие настроек средств защиты информации требованиям проектной и эксплуатационной документации на подсистему обеспечения информационной безопасности (в случае наличия), эксплуатационной документации на средства защиты информации или рекомендациям производителя средств защиты информации;

– проверка наличия актуальных (последних выпущенных производителем на момент проведения проверки) баз сигнатур средств защиты информации, предусматривающих использование баз сигнатур (антивирусных средств, средств анализа (контроля) защищенности, обнаружения вторжений);

– анализ состава и содержания событий, зарегистрированных в журналах регистрации событий средств защиты информации;

– контроль целостности программного обеспечения средств защиты информации;

– выборочное тестирование выполнения средствами защиты информации своих функций.

Дополнительно в рамках проверки корректности функционирования средств защиты осуществляется проверка корректности правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей и реализации правил разграничения доступа, выполняемых средствами защиты информации от несанкционированного доступа из состава подсистемы обеспечения информационной безопасности.

Результаты проверки корректности настроек и функционирования средств защиты информации включаются в Журнал учета мероприятий по контролю защищенности.

8.3.3. Проверка выполнения организационных мер защиты информации

Проверка фактического выполнения организационных мер защиты производится путем выборочных проверок выполнения организационных мер защиты и требований организационно-распорядительных документов в области защиты информации.

Результаты проверок включаются в Журнал учета мероприятий по контролю защищенности.

8.3.4. Анализ уязвимостей

Анализ уязвимостей производится с использованием инструментальных средств анализа защищенности, входящего в состав подсистемы обеспечения информационной безопасности ИС. Анализ уязвимостей ИС проводится не реже одно раза в квартал.

Конкретный перечень проверок устанавливается Администратором информационной безопасности и уточняется с периодичностью не реже раза в год, либо в случае появления информации о новых уязвимостях.

Дополнительно проводится поиск известных (опубликованных в открытых источниках, в том числе в базе данных угроз безопасности ФСТЭК России) уязвимостей в системном и прикладном программном обеспечении ИС, а также программном и(или) микропрограммном обеспечении базовой системы ввода-вывода, средств защиты информации и сетевого оборудования.

Доступ к функционалу средства анализа защищенности по выявлению (поиску) уязвимости предоставляется только администратору информационной безопасности.

Анализ уязвимостей может осуществляться сотрудниками (служащими) юридического лица, которому функции по обеспечению информационной безопасности делегированы со стороны Учреждения на основании договора.

При выявлении (поиске), анализе и устранении уязвимостей проводится:

– выявление (поиск) уязвимостей, связанных с правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;

– разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей;

– анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;

– перечень полученных уязвимостей, при наличии возможности, должен быть устранен Администратором информационной безопасности в течении 1 (одного) года путем установки обновлений программного обеспечения, выпущенных производителем программного обеспечения.

В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения, Администратор информационной безопасности должен предпринять действия (настройки средств защиты информации, изменение режима и порядка использования информационной системы), направленные на устранение возможности использования выявленных уязвимостей.

Выводы, основанные на данных, полученных в результате анализа уязвимостей, включаются в Журнал учета мероприятий по контролю защищенности.

Выявленные уязвимости должны быть оперативно устранены путем выполнения рекомендаций разработчика программного обеспечения.

8.3.5. Проверка неизменности программно-аппаратной инфраструктуры

В рамках проверки неизменности программно-аппаратной инфраструктуры ИС Учреждения выполняется сравнение фактического состава и размещения технических средств и программного обеспечения со сведениями, приведенными в техническом паспорте.

В случае выявления несоответствия фактического состава и размещения технических средств и программного обеспечения сведениям, приведенным в техническом паспорте, данные факты включаются в Журнал учета мероприятий по контролю защищенности.

9. Защита машинных носителей информации

9.1 Носители информации

В настоящем Положении рассматриваются следующие виды материальных носителей информации:

- машинные носители информации;
- носители информации на бумажной основе.

Машинные носители информации – изделия и устройства, предназначенные для записи и обработки информации в составе средств вычислительной техники, а также для хранения и перемещения записанной информации за пределы состава средств вычислительной техники.

К МНИ относятся:

- жесткие магнитные диски;
- оптические и магнитооптические диски;
- устройства долговременной электронной памяти «Flash Memory»;
- магнитные ленты.

Машинные носители бывают следующих типов:

- съемные – носители информации устанавливаются и/или подключаются к средствам вычислительной техники на время сеанса работы пользователя, а по окончании его отключаются и хранятся в оборудованном хранилище;
- несъемные – носитель информации в процессе работы пользователя не

снимается и не изымается из состава средств вычислительной техники автоматизированной системы и находится там постоянно.

Носители информации на бумажной основе – материальные носители графической и буквенно-цифровой информации, отраженной (зафиксированной) на бумаге.

9.2 Учет машинных носителей информации

В Учреждении запрещено использование (находящихся в личном использовании) съемных машинных носителей информации и съемных машинных носителей информации, для которых не определен владелец (пользователь, ответственные за принятие мер защиты информации).

В ИС Учреждения все МНИ подлежат учету в Журнале учета машинных носителей информации (форма журнала установлена в Приложении № 8).

Учет МНИ включает присвоение регистрационных (учетных) номеров носителям.

В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, и (или) номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации.

На жестких магнитных дисках и внешних накопителях (USB и т.п.) штамп (форма штампа установлена в Приложении № 9) проставляется на этикетке, закрепленной с помощью липкой ленты на лицевой стороне носителя.

На несъёмных носителях информации штамп ставится на корпусе системного блока АРМ в котором установлен носитель. Несъемные жесткие магнитные диски учитываются отдельно и (или) в составе системного блока АРМ. Системный блок АРМ для маркировки и контроля его наличия вскрывается в присутствии ответственного за его эксплуатацию, а для АРМ, находящегося на гарантийном или после гарантийном обслуживании, кроме того и в присутствии (с разрешения) представителя обслуживающей организации.

После вскрытия, маркировки или контроля ее наличия системный блок должен быть надёжно опечатан, подписями ответственного за АРМ и Администратора информационной безопасности.

Учет МНИ осуществляется администратором информационной безопасности с использованием Журнала учета машинных носителей информации. Допускается ведение журнала в электронном виде. Ответственность за ведение журнала возлагается на Администратора информационной безопасности.

Учет встроенных в портативные или стационарные технические средства машинных носителей информации может вестись в журналах материально-технического учета в составе соответствующих технических средств.

При использовании в составе одного технического средства нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

Регистрационные или иные номера подлежат занесению в Журнал учета машинных носителей информации или журналы материально-технического учета с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации.

9.3 Управление доступом к машинным носителям информации

Физический доступ к МНИ должен быть ограничен перечнем лиц, которым он необходим для выполнения своих должностных обязанностей (функций).

Администратором информационной безопасности производится опечатывание корпусов средств вычислительной техники, в которых стационарно установлены машинные носители информации, опечатывающим материалом, исключающим возможность скрытия факта нарушения целостности.

В случае выявления фактов несанкционированного нарушения целостности опечатывающего материала либо выявления иных следов

несанкционированного вскрытия корпусов средств вычислительной техники, администратор информационной безопасности должен действовать согласно пункту 5 настоящего Положения.

Защищаемые носители информации выдаются пользователям под расписку в Журнале учета машинных носителей информации или если носитель выдается временно на срок не более трех дней, по лицевому счету (форма лицевого счета установлена в Приложении № 10).

В случае служебной необходимости (отпуск, увольнение, перевод и т.п.) защищаемый носитель может быть передан другому пользователю. Передача носителя другим пользователям осуществляется через журнал учета машинных носителей информации или через лицевые счета.

В ходе обратного приёма проверяются учётные данные передаваемого носителя – производитель, модель и серийный номер. По результатам проверки Администратором информационной безопасности делается отметка в графе обратного приёма.

Уборка и технические работы в помещениях, в которых установлены автоматизированные рабочие места с защищаемыми носителями, производятся в присутствии одного из должностных лиц, допущенных в указанное помещение установленным порядком.

9.4 Хранение защищаемых носителей

При хранении защищаемых носителей информации должны соблюдаться условия, обеспечивающие сохранность конфиденциальной информации и исключающие несанкционированный к ним доступ, исключающие хищение, подмену и уничтожение.

Хранение защищаемых носителей информации должно осуществляться в условиях, соответствующих техническим условиям их заводов-изготовителей.

Недопустимо воздействие на защищаемых носители информации теплового, светового (ультрафиолетового) и ионизирующего излучений. Также недопустимо размещение мест хранения защищаемых носителей информации

вблизи источников электромагнитных колебаний (телефоны, электродвигатели, кабели и т.п.).

Необходимо обеспечивать раздельное хранение информации (материальных носителей информации на бумажной основе), обработка которых осуществляется в различных целях. Для хранения защищаемых носителей информации используются специально оборудованные хранилища (сейфы, шкафы, и т.п.), исключающие возможность несанкционированного копирования информации и хищения носителей.

Защищаемые носители с резервными копиями информации не выдаются для работы обычным пользователям и служат только для восстановления информации в случае аварии или поломки основного носителя информации. Защищаемые носители с резервными копиями информации рекомендуется хранить в отдельном хранилище.

В случае, если Учреждение на основании договора поручает хранение машинных носителей информации другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности информации и безопасности информации при их хранении.

9.5 Уничтожение информации на машинных носителях и контроль их перемещения

Уничтожение (стирание) информации с машинных носителей информации производится путем перезаписи уничтожаемых (стираемых) файлов случайной битовой последовательностью, удаления записи о файлах, обнуления журнала файловой системы или полной перезаписи всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием.

Освобождаемые области оперативной памяти АРМ и внешних накопителей подвергаются очистке (обнулению, обезличиванию).

Уничтожение (стирание) информации с машинных носителей информации должно производиться обязательно в следующих случаях:

– перед первичным подключением машинных носителей информации к

средствам вычислительной техники из состава ИС Учреждения;

– при достижении целей обработки информации или в случае утраты необходимости в их достижении;

– в случаях выноса машинных носителей информации за пределы контролируемой зоны, в том числе в рамках передачи в специализированные организации для ремонта, гарантийного обслуживания, утилизации или с иными целями.

Машинные носители информации (отдельно или в составе средств вычислительной техники) запрещается перемещать за пределы контролируемой зоны за исключением случаев, требующих их ремонта или утилизации.

В случае, если произвести уничтожение (стирание) информации с машинных носителей информации не представляется возможным, машинный носитель информации должен быть уничтожен путем физического разрушения, исключающего возможность его ремонта и повторного использования, а также восстановления с него информации специально предназначенными для этого средствами.

Машинный носитель информации также уничтожается в случае выхода из строя или повреждения носителя информации, в результате которого невозможно осуществлять корректную обработку информации с использование данного носителя. По результатам уничтожения машинного носителя информации может составляться акт об уничтожении. Акты сдаются на хранение Администратору информационной безопасности. Срок хранения актов- не менее одного года. Факт об уничтожении машинного носителя отражается в журнале учета машинных носителей информации.

10. Антивирусная защита информации

10.1 Общие требования

К использованию в составе компонента антивирусной защиты допускаются только сертифицированные антивирусные средства с действующим сертификатом соответствия ФСТЭК России и/или ФСБ России.

Настройка параметров средств антивирусного контроля осуществляет администратор информационной безопасности в соответствии с руководствами по применению конкретных антивирусных средств.

10.2 Применение средств антивирусного контроля

Перед загрузкой дистрибутивов и обновлений (патчей) программного обеспечения в ИС Учреждения должна быть проведена их антивирусная проверка с использованием средства антивирусной защиты.

Ежедневно перед началом работы после загрузки операционной системы (ОС) на рабочих станциях пользователей ИС Учреждения в автоматическом режиме должен проводиться антивирусный контроль всех используемых для работы носителей информации (дисков и файлов). Антивирусный контроль серверного оборудования Учреждения должен происходить еженедельно.

Пользователи ИС при работе с носителями информации обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов. Ярлык для запуска антивирусной программы должен быть вынесен на «Рабочий стол» операционной системы.

Доступ к администрированию средств антивирусной защиты предоставляется только Администратору информационной безопасности ИС Учреждения. Доступ к консоли управления антивирусным средством должен ограничиваться паролем с учетом требований парольной политики.

Пользователям запрещается отключать АВПО и самостоятельно вносить изменения в их настройки. Управление АВПО может осуществляться централизованно.

Средство антивирусной защиты должно быть настроено таким образом, в автоматическом режиме производился периодический антивирусный контроль объектов ИС (автоматизированных рабочих мест, серверов, других средств вычислительной техники), а также проверка в режиме времени близком к реальному объектов (файлов), которые попадают из внешних источников (съемных машинных носителей информации, сетевых подключений и других

внешних источников) при загрузке, открытии или исполнении таких файлов на наличие вредоносных компьютерных программ (вирусов).

Обязательному входному антивирусному контролю подлежит любая информация, поступающая на средства вычислительной техники, программные средства общего и специального назначения, любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по каналам передачи данных, а также информация на съемных машинных носителях информации (CD-ROM, Flash-накопителях и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед ее отправкой (записью на съемный машинный носитель информации).

Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц. Периодическая проверка жестких магнитных дисков на отсутствие программных вирусов должна проводиться не реже одного раза в неделю.

При повреждении программных средств и информационных массивов программными вирусами должны выполняться мероприятия по восстановлению их работоспособности.

10.3 Действия персонала при обнаружении компьютерного вируса

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов, пользователи обязаны немедленно оповестить Администратора информационной безопасности и прекратить какие-либо действия на своем АРМ.

Администратор информационной безопасности проводит расследование факта заражения АРМ пользователя (или сервера ИС) компьютерным вирусом. Лечение зараженных файлов осуществляется путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводится антивирусный контроль.

В случае обнаружение нового вируса, не поддающегося лечению средствами антивирусной защиты администратор информационной безопасности должен:

– заархивировать зараженные файлы с внедренными программными вирусами и направить данный архив в организацию, с которой заключен договор технической поддержки эксплуатации средств антивирусной защиты (в случае наличия такого договора);

– осуществить удаление вирусной программы и нейтрализации последствий вирусного заражения.

Обо всех фактах заражения Администратор информационной безопасности обязан ставить в известность руководство Учреждения.

Установка и настройка параметров средства антивирусной защиты на средствах вычислительной техники Учреждения осуществляется в соответствии с программной и эксплуатационной документацией, поставляемой вместе со средством антивирусной защиты.

10.4 Порядок обновления антивирусных баз

Обновление антивирусных баз должно проводиться регулярно, в автоматическом режиме, по мере выхода новых антивирусных баз.

Периодический контроль за состоянием антивирусной защиты, а также за соблюдение установленного порядка антивирусного контроля возлагается на Администратора информационной безопасности.

Источниками обновлений могут являться:

– серверы обновлений производителей АВПО;

– зеркальный сервер, созданный Администратором информационной безопасности внутри локальной вычислительной сети Учреждения.

Для автономных рабочих мест, не имеющих доступ в сеть Интернет или подключение к локально-вычислительной сети Учреждения обновление антивирусных баз производится локально администратором информационной безопасности по мере выхода новых антивирусных баз.

Запрещается устанавливать обновления ядра АВПО.

11. Обнаружение вторжений

При необходимости в Учреждении могут применяться меры по обнаружению вторжений. Обнаружение вторжений должно осуществляться на внешней границе ИС Учреждения (системами обнаружения вторжений уровня сети) и (или) на технических средствах (системами обнаружения вторжений уровня узла) ИС (автоматизированных рабочих местах, серверах и иных технических средствах).

Применяемые системы обнаружения вторжений должны включать компоненты регистрации событий безопасности (датчики), компоненты анализа событий безопасности и распознавания компьютерных атак (анализаторы), а также базу решающих правил, содержащую информацию о характерных признаках компьютерных атак.

Настройки средств обнаружения вторжений должны позволять автоматически реагировать на вторжения в ИС Учреждения.

Права по управлению (администрированию) системами обнаружения вторжений должны быть представлены только Администратору информационной безопасности.

Обновление базы решающих правил системы обнаружения вторжений должно предусматривать:

– получение уведомлений о необходимости обновлений и непосредственном обновлении базы решающих правил;

– получение и установку обновлений базы решающих правил только из доверенных источников;

– контроль целостности обновлений базы решающих правил.

Уведомления от системы обнаружения вторжений должны автоматически оповещать администратора информационной безопасности о необходимости обновления баз решающих правил.

Администратором информационной безопасности должно обеспечиваться обновление базы решающих правил системы обнаружения вторжений, применяемой в ИС Учреждения по мере выпуска производителем системы обновлений баз решающих правил. Перед обновлением баз решающих правил Администратор информационной безопасности обязан сохранить в резервном файле настройки конфигурации технического средства или ПО, реализующего функции средства обнаружения вторжений.

12. Резервное копирование и восстановление информации

12.1 Информационные ресурсы, подлежащие резервированию

Резервному копированию подлежат все информационные ресурсы Учреждения, содержащие конфиденциальную и защищаемую информацию, например:

– файлы баз данных;

– электронные документы;

– СУБД;

– конфигурация необходимого для работы в ИС ПО и средств защиты информации;

– журналы аудита событий безопасности;

– иная информация ИС.

Резервированию могут подлежать также технические средства, программное обеспечение и каналы передачи информации, средства функционирования информационной системы, при этом:

– резервные компоненты технических средств и каналов связи находятся в выключенном состоянии. При выходе из строя какого-либо из основных компонентов его заменяет резервный, приведенный в соответствие текущим настройкам системы;

– резервирование программного обеспечения выполняется путем резервирования ПО серверов и АРМ на архивный дисковый массив, сетевое хранилище и т.д.

С целью предотвращения потери защищаемой информации в Учреждении должно быть реализовано резервное копирование баз данных информационных ресурсов серверов систем управления базами данных.

В отношении информации, хранящейся в электронных журналах аудита событий безопасности, должна быть организована процедура архивации данных по расписанию и по вызову специальной команды.

Носители, на которые произведено резервное копирование, должны быть учтены и пронумерованы: номером носителя, датой проведения резервного копирования.

12.2 Порядок резервирования

Резервирование информационных ресурсов ИС выполняется Администратором информационных систем.

Определяется 2 вида резервирования:

– полное резервирование – резервное копирование всей информации, хранящейся в ИС;

– неполное резервирование информации – резервное копирование части, хранящейся в ИС.

Целью неполного резервирования является сохранение изменений в ИС с момента полного резервирования.

Периодичность проведения работ по резервированию определяется администратором информационных систем с учётом специфики работы ИС, но не менее 1 раза в месяц для полного резервирования и 1 раза в неделю для неполного резервирования.

В случаях, когда информационные ресурсы хранятся на АРМ пользователей локально, допустимо перекладывать ответственность за проведение неполного резервирования на пользователей ИС.

События резервирования фиксируются в «Журнале резервирования информационных ресурсов ИС» (форма журнала установлена в Приложении № 11). В журнале указывается: дата, вид резервирования, наименование

резервируемого информационного ресурса, количество и общий размер файлов, серийный номер носителя информации, ответственное лицо.

Администратор информационных систем использует средства резервного копирования для резервирования информации на выделенный носитель информации. Резервное копирование с использованием незащищённых каналов связи общего пользования не допустимо.

Администратор информационных систем не имеет право ознакамливаться с резервируемой информацией. Факт ознакомления администратора информационных систем с резервируемой информацией может быть расценён как превышение служебных полномочий в соответствии с Трудовым Кодексом Российской Федерации и Кодексом об Административных Правонарушениях Российской Федерации.

При резервировании информации не допускается хранение на одном носителе резервных копий, извлечённых из различных ИС. Для осуществления резервирования различных ИС, для каждой ИС должен быть предусмотрен отдельный носитель информации или электронная папка.

В случае удаления информации из ИС должна быть так же удалена резервная копия этих данных.

Резервное копирование программных компонентов средств защиты информации и их настроек должно осуществляться путем ведения двух копий программных компонентов средств защиты информации и настроек СЗИ, периодического обновления СЗИ и контроля работоспособности.

12.3 Хранение резервных копий

Хранение резервных копий должно исключать любой несанкционированный доступ посторонних лиц к носителям информации.

Хранение материальных носителей, содержащих резервные копии необходимо осуществлять в сейфах, несгораемых шкафах, металлических шкафах с устройством опечатывания. Доступ к местам хранения резервных копий должен быть предоставлен только администратору информационных

систем и ответственному за организацию обработки конфиденциальной информации (или персональных данных).

На носителе информации, содержащем резервные копии, не должна храниться посторонняя информация.

12.4 Порядок восстановления информации после сбоя

В случае сбоя в работе ИС, восстановление информации из резервных копий осуществляет администратор информационных систем.

Факты восстановления информации должны фиксироваться в «Журнале резервирования информационных ресурсов» (в графе «вид резервирования» указывается «полное восстановление» либо «частичное восстановление»).

Восстановление информации должно быть произведено в кратчайшие сроки (по возможности в срок не превышающий одного рабочего дня).

13. Взаимодействие с внешними информационными системами

Взаимодействие ИС Учреждения с внешними ИС может производиться с целью обмена информацией. Взаимодействие ИС Учреждения с внешними информационными системами осуществляется при выполнении следующих условий:

– при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней системы;

– при наличии подтверждения выполнения во внешней ИС, предъявленных к ней требований по защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

В договоре об информационном взаимодействии должны быть согласованы количество пользователей, определены типы подключения и типы прикладного ПО ИС Учреждения к которым предоставляется доступ авторизованным пользователям из внешних ИС, определены необходимые системные учетные записи. Взаимодействие между ИС должно осуществляться по защищенным каналам связи.

14. Обеспечение безопасности удаленного доступа

14.1 Организация удаленного доступа

Под удаленным доступом к ресурсам ИС Учреждения все виды доступа, осуществляемые по внешним каналам связи и с использованием устройств доступа, расположенных за пределами контролируемой зоны.

Удаленный доступ к ресурсам ИС Учреждения может быть предоставлен как внешним пользователям, так и сотрудникам Учреждения. Представление удаленного доступа внешним пользователя производится согласно п. 12 настоящего Положения на основании Договора.

Предоставление удаленного доступа сотруднику Учреждения должно быть обосновано производственной необходимостью. Удаленный доступ сотрудников к ресурсам ИС предоставляется только на основании заявки (форма заявки установлена в Приложении № 12) и прохождения специального инструктажа, проводимого Администратором информационной безопасности.

Сотрудники Учреждения, которым предоставляется удаленный доступ, несут персональную ответственность за использование предоставляемого доступа только по назначению с соблюдением требований безопасности информации, устанавливаемых настоящим Положением и иными внутренними нормативными документами Министерства. Удаленный доступ предоставляется только по защищенным каналам связи, для подтверждения подлинности удаленных пользователей могут применяться одноразовые пароли, криптографические ключи и методы многофакторной аутентификации.

Сотрудники, получившие удалённый доступ, обязаны принимать меры по недопущению использования своих устройств, с которых происходит удаленный доступ посторонними лицами для осуществления удаленного доступа к ресурсам ИС.

14.2 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные системы

Защита удаленного доступа должна обеспечиваться при всех видах доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа) и должна включать:

– ограничение на использование удаленного доступа в соответствии с задачами (функциями) ИС, для решения которых такой доступ необходим, и предоставление удаленного доступа для каждого разрешенного вида удаленного доступа;

– предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);

– мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа ИС;

– контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа ИС до начала информационного взаимодействия с ИС (передачи защищаемой информации).

Для вышеприведенных мер защиты удаленного доступа, в Учреждении могут применяться специальные автоматизированные средства.

15. Защита виртуальной инфраструктуры

15.1 Понятие виртуальной инфраструктуры и идентификация и аутентификация

При применении в Учреждении технологий виртуализации и обработки информации внутри виртуальной инфраструктуры должны быть приняты меры по ее защите.

Для защиты виртуальной инфраструктуры в Учреждении должны применяться специальные сертифицированные средства защиты виртуальной инфраструктуры (далее – средства защиты ВИ). Средствами защиты ВИ должна обеспечиваться идентификация и аутентификация субъектов доступа и объектов доступа, в том числе администраторов управления средствами виртуализации.

Виртуальная инфраструктура включает в себя среду виртуализации (ПО, служебные данные компонентов виртуальной инфраструктуры) и аппаратное обеспечение (аппаратные средства, необходимые для функционирования среды виртуализации).

В качестве компонентов виртуальной инфраструктуры рассматривается серверное оборудование, аппаратное обеспечение консолей управления, оборудование хранения данных, сетевое оборудование, гипервизор, хостовая ОС (если применимо), виртуальные машины, программная среда виртуальных машин (в том числе их ОС и ПО), виртуальное аппаратное обеспечение, виртуализированное ПО (виртуальные машины с предустановленным ПО, предназначенным для выполнения определенных функций в виртуальной инфраструктуре), ПО управления виртуальной инфраструктуры (в том числе гипервизором, настройками виртуальных машин, миграцией виртуальных машин, балансировкой нагрузки), служебные данные компонентов виртуальной инфраструктуры (настройки и иные служебные данные) и средства защиты информации, используемые в рамках виртуальных машин и виртуальной инфраструктуры в целом.

В качестве объектов доступа в виртуальной инфраструктуре рассматривается ПО управления ВИ, гипервизор, хостовая ОС (если применимо), виртуальные машины, программная среда виртуальных машин (в том числе их ОС и ПО), виртуальные контейнеры (зоны), виртуализированное ПО (виртуальные машины с предустановленным ПО, предназначенная для выполнения определенных функций в виртуальной инфраструктуре), средства защиты информации, используемые в рамках виртуальных машин и в виртуальной инфраструктуре в целом.

При реализации мер по идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре должно обеспечиваться:

– идентификация и аутентификация администраторов управления средствами виртуализации;

– идентификация и аутентификация субъектов доступа при их локальном и удалённом обращении к объектам доступа в виртуальной инфраструктуре;

– блокировка доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

– защита аутентификационной информации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерного доступа к ней, уничтожения или модифицирования;

– защита аутентификационной информации в процессе ее ввода для аутентификации в виртуальной инфраструктуре от возможного использования лицами, не имеющими на это полномочий;

– идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления параметрами аппаратного обеспечения виртуальной инфраструктуры.

Внутри развернутых на базе виртуальной инфраструктуры виртуальных машин обеспечивается реализация мер по идентификации и аутентификации субъектов и объектов доступа, в том числе путем установки и настройки средств защиты информации.

В ИС должна обеспечиваться взаимная идентификация и аутентификация пользователя и сервера виртуализации (виртуальных машин) при удалённом доступе.

15.2 Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре

При реализации процедур по идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре должны обеспечиваться:

– идентификация и аутентификация администраторов управления средствами виртуализации;

– идентификация и аутентификация субъектов доступа при их локальном и удалённом обращении к объектам доступа в виртуальной инфраструктуре;

– блокировка доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

– защита аутентификационной информации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерного доступа к ней, уничтожения или модифицирования;

– защита аутентификационной информации в процессе ее ввода для аутентификации в виртуальной инфраструктуре от возможного использования лицами, не имеющими на это полномочий;

– идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления параметрами аппаратного обеспечения виртуальной инфраструктуры.

При реализации правил по управлению доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре должны обеспечиваться:

– контроль доступа субъектов доступа к средствам управления компонентами виртуальной инфраструктуры;

– контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения, виртуальных машин, файлам-образам, служебным данным, используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды;

– управление доступом к виртуальному аппаратному обеспечению информационной системы, являющимся объектом доступа;

– контроль запуска виртуальных машин на основе заданных оператором правил (режима запуска, типа используемого носителя и иных правил).

15.3 Правила и процедуры регистрация событий безопасности в виртуальной инфраструктуре

При реализации процедур по регистрации событий безопасности в виртуальной инфраструктуре дополнительно к событиям, установленным в

разделе 3 настоящего Положения, должны подлежать регистрации следующие события:

– запуск (завершение) работы компонентов виртуальной инфраструктуры;

– доступ субъектов доступа к компонентам виртуальной инфраструктуры;

– изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения;

– изменения правил разграничения доступа к компонентам виртуальной инфраструктуры.

15.4 Рекомендации по управлению (разделению) потоков информации между компонентами виртуальной среды

В ИС Учреждения, с технологией виртуализации, Администратором информационной безопасности должна обеспечиваться единая точка подключения к виртуальной инфраструктуре (при необходимости резервирования каналов связи, точка подключения должна рассматриваться как комплексное решение, включающее в себя средства взаимодействия с основным и резервными каналами связи).

Администратор информационной безопасности должен обеспечивать фильтрацию сетевого трафика от (к) каждой гостевой операционной системы, в виртуальных сетях гипервизора и для каждой виртуальной машины.

При реализации правил по управлению потоками информации между компонентами виртуальной инфраструктуры должны обеспечиваться:

– фильтрация сетевого трафика между компонентами виртуальной инфраструктуры, в том числе между внешними по отношению к серверу виртуализации сетями и внутренними по отношению к серверу виртуализации сетями, в том числе при организации сетевого обмена с сетями связи общего пользования;

– обеспечение доверенных канала, маршрута внутри виртуальной инфраструктуры между администратором, пользователем и средствами защиты информации (функциями безопасности);

– контроль передачи служебных информационных сообщений, передаваемых в виртуальных сетях гипервизора, хостовой операционной системы, по составу, объёму и иным характеристикам;

– отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры гипервизора, хостовой операционной системы, виртуальной вычислительной сети;

– обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;

– обеспечение изоляции потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры (гипервизором, хостовой операционной системой) и сетевых потоков виртуальной вычислительной сети;

– семантический и статистический анализ сетевого трафика виртуальной вычислительной сети.

15.5 Порядок контроля резервирования, целостности и перемещения виртуальных машин и обрабатываемой информации

В ИС Учреждения Администратор информационной безопасности обеспечивает контроль резервирования и целостности компонентов виртуальной инфраструктуры.

Администратор информационной безопасности обеспечивает контроль целостности резервных копий виртуальных машин (контейнеров).

При реализации порядка контроля целостности компонентов виртуальной инфраструктуры должны обеспечиваться:

– контроль целостности состава и конфигурации виртуального оборудования;

– контроль целостности компонентов, критически важных для функционирования хостовой ОС, гипервизора, гостевых ОС и (или) обеспечения безопасности, обрабатываемой в них информации (загрузчика, системных файлов, библиотек операционной системы и иных компонентов);

– контроль целостности файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин;

– контроль целостности базовой системы ввода-вывода вычислительных серверов и консолей управления виртуальной инфраструктуры;

– контроль состава аппаратной части компонентов виртуальной инфраструктуры;

– контроль целостности файлов-образов виртуализированного ПО и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем (контроль файлов-образов должен проводиться во время, когда файлы-образы не задействованы).

В ИС Учреждения Администратором информационной безопасности обеспечивается перемещение виртуальных машин (контейнеров) и обрабатываемых на них данных в пределах информационной системы только на контролируемые им (или уполномоченным лицом) технические средства (сервера виртуализации, носители, системы хранения данных).

Администратор информационной безопасности осуществляет обработка отказов перемещения виртуальных машин (контейнеров) и обрабатываемых на них данных.

При перемещении виртуальных машин (контейнеров) и обрабатываемой информации должны обеспечиваться:

– регламентирование порядка перемещения (определение ответственных за организацию процесса, объектов перемещения, ресурсов инфраструктуры, задействованных в перемещении, а также способов перемещения);

– управление размещением и перемещением исполняемых виртуальных машин (контейнеров) между серверами виртуализации;

– управление размещением и перемещением файлов-образов виртуальных машин (контейнеров) между носителями (системами хранения данных);

– управление размещением и перемещением данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных).

Управление перемещением виртуальных машин (контейнеров) предусматривает:

– полный запрет перемещения виртуальных машин (контейнеров);

– ограничение перемещения виртуальных машин (контейнеров) в пределах информационной системы (сегмента информационной системы);

– ограничение перемещения виртуальных машин (контейнеров) между сегментами информационной системы.

16. Правила и процедуры защиты мобильных технических средств

К мобильным техническим средствам, в рамках настоящего Положения, относятся портативные вычислительные устройства и устройства связи с возможностью обработки информации (например: ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные средства).

Мобильные технические средства, используемые в ИС должны рассматриваться как отдельный сегмент ИС (мобильный сегмент).

В качестве мер обеспечения безопасности информации, обрабатываемой в мобильном сегменте должны быть реализованы, в том числе, следующие меры:

– очистка (удаление) информации в мобильном техническом средстве после завершения сеанса удаленного доступа к защищаемой информации или принятие иных мер, исключающих несанкционированный доступ к хранимой защищаемой информации;

– уничтожение съемных машинных носителей информации, которые не подлежат очистке;

– выборочные проверки мобильных технических средств (на предмет их наличия) и хранящейся на них информации (например, на предмет отсутствия информации, не соответствующей маркировке носителя информации).

Запрет возможности автоматического запуска (без команды пользователя) в ИС ПО на мобильных технических средствах.

На мобильном техническом средстве (в зависимости от типа) должны быть реализованы меры по защите информации (идентификация, аутентификация, управление доступом, антивирусная защита и т.д).

Администратором информационной безопасности периодически должны проводится работы по мониторингу и контролю применения мобильных технических средств на предмет выявления несанкционированного использования таких средств, а также реализованных мер защиты информации на мобильных технических средствах.

17. Правила и процедуры применения технологий беспроводного доступа

В ИС Учреждения устанавливается возможность использования технологий беспроводного доступа (исходя из технологического процесса обработки информации), что должно быть отражено в технической документации на ИС. Решение по использованию в ИС технологий беспроводного доступа определяется Администратором информационных систем и оценивается Администратором информационной безопасности.

В случае запрета использования технологий беспроводного доступа, Администратор информационных систем обеспечивает его запрет при помощи имеющейся инфраструктуры и средств защиты информации.

В пределах контролируемой зоны допускается устанавливать средства беспроводного доступа, физически либо логически отделенные от ИС, при этом должны быть выполнены следующие условия:

– получено разрешение от Администратора информационной безопасности на размещение средства беспроводного доступа;

– Администратором ИБ должны быть установлены безопасные настройки средства беспроводного доступа.

Создание беспроводных точек доступа возможно только по согласованию с Администратором информационной безопасности, осуществляется на основании письменного запроса, подписанного руководителем структурного подразделения, в котором планируется создание таких точек, содержащего обоснование необходимости создания беспроводной точки подключения.

Защита беспроводных точек доступа при подключении вариантом hot-spot (через точку доступа) следующими механизмами:

– блокировка широковещательных передач узлом доступа (режим скрытого идентификатора сети);

– фильтрация доступа клиентов сети по MAC-адресам по «белому списку»;

– использование сложного ключа доступа к сети (более 8 символов, отвечает требованиям к сложности, периодическая смена и др.);

– использование в качестве метода аутентификации и шифрования технологию WPA. Рекомендуется применять технологию WPA корпоративного уровня (WPA 2 Enterprise).

18. Правила и процедура управления информационными потоками между устройствами

В ИС Учреждения Администратором информационной безопасности должно обеспечиваться управление информационными потоками при передаче информации между устройствами, сегментами в рамках ИС. Управление потоками может осуществляться путем применения средств межсетевого экранирования. Для каждого устройства, сегмента ИС Администратор информационной безопасности определяет минимальный набор правил фильтрации, необходимость ограничивать информационные потоки, необходимость записи во временное хранилище информации для анализа и принятия решений о возможности ее дальнейшей передачи.

При установлении правил фильтрации должен быть обеспечен принцип «Запрещено всё, кроме разрешенного», например, при формировании правил фильтрации основным правилом фильтрации должен быть «запрещены любые сетевые пакеты в любом направлении».

19. Правила защиты ИС, ее средств, систем связи и передачи данных

В ИС осуществляется разделение полномочий на администраторские и пользовательские. Пользовательские полномочия (права) используются исключительно для обработки информации, администраторские полномочия (права) используются исключительно для настройки параметров ОС, ПО и средств защиты информации.

Использование технологии мобильного кода (Java, JavaScript, ActiveX, PDF, Postscript, Flash-анимация, VBScript и т.п.) разрешается исключительно в служебных целях.

19.1 Правила и процедуры обеспечения защиты информации при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны

Защита систем связи и передачи данных заключается в обеспечении безопасности защищаемой информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.

Запрещается передача защищаемой информации по открытым каналам связи за пределы контролируемой зоны без применения сертифицированных по требованиям безопасности средств криптографической защиты информации (СКЗИ).

19.2 Правила и процедуры применения видеокамер, микрофонов и иных периферийных устройств

В ИС запрещено применение видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно или которые имеют возможность управления через компоненты программного обеспечения, установленных на рабочем месте пользователя, коммуникационных сервисов сторонних лиц (провайдеров) (ICQ, Skype и иные сервисы).

20. Обеспечение безопасности информации в ходе эксплуатации ИС Учреждения

20.1 Планирование мероприятий по защите информации в ИС Учреждения

Ответственным за планирование мероприятий по защите информации, обрабатываемой в ИС Учреждения, является администратор информационной безопасности.

Контроль исполнения плана мероприятий по защите информации в ИС Учреждения осуществляет Ректор Учреждения.

Администратор информационной безопасности разрабатывает годовой план мероприятий по защите информации, обрабатываемой в ИС Учреждения, и согласует его с руководителями подразделений, непосредственно реализующих обработку информации в ИС Учреждения или участвующими в реализации мероприятий. Согласованный план направляется на утверждение генеральному директору Учреждения не позднее 30 ноября года, предшествующему планируемому периоду.

План мероприятий по защите информации, обрабатываемой в ИС Учреждения, подлежит актуализации ежеквартально на основании текущего состояния ПОИБ ИС Учреждения, изменений в правовые и нормативные документы, регулирующие защиту информации. Внесение изменений в план мероприятий по защите информации, обрабатываемой в ИС Учреждения, может быть инициировано по результатам реагирования на инциденты безопасности

информации, на основании предписаний органов исполнительной власти, уполномоченных в области защиты информации,

Контроль выполнения мероприятий по обеспечению защиты информации в ИС Учреждения, предусмотренных утвержденным планом, осуществляется генеральным директором Учреждения на основании ежеквартальных отчетов администратора информационной безопасности.

20.2 Информирование и обучение пользователей ИС Учреждения

Ответственным за информирование и обучение пользователей по вопросам обеспечения информационной безопасности является Администратор информационной безопасности, который самостоятельно или совместно с организацией, обладающей соответствующими лицензиями, обеспечивает:

– информирование пользователей ИС Учреждения о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации ИС Учреждения – по мере выявления актуальных угроз;

– доведение до пользователей ИС Учреждения требований по защите информации, а также положений организационно-распорядительных документов по защите информации с учетом внесенных в них изменений – по мере внесения изменений в организационно-распорядительные документы по защите информации;

– обучение пользователей ИС Учреждения правилам эксплуатации отдельных средств защиты информации – в ходе первичного инструктажа пользователей при предоставлении доступа к ИС Учреждения или при внесении изменений в конфигурацию ПОИБ ИС Учреждения, изменяющих правил (приемов) использования средств защиты;

– проведение практических занятий и тренировок с пользователями ИС Учреждения по блокированию угроз безопасности информации и реагированию на инциденты – регулярно, не реже, чем 1 раз квартал или по мере выявления инцидентов или актуальных угроз;

– контроль осведомленности пользователей ИС Учреждения об угрозах

безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации – по завершению инструктажей, занятий, тренировок.

В Учреждении в качестве форматов обучения по вопросам информационной безопасности определены следующие форматы:

- полные курсы (длительностью 5 дней и более);
- кратковременные курсы (длительностью от 1 до 3 дней);
- внешние и внутренние семинары;
- конференции;
- инструктажи.

Полные и кратковременные курсы, конференции, внешние семинары проводятся во внешних специализированных организациях для следующих категорий ответственных лиц:

- ответственный за организацию обработки конфиденциальной информации (или персональных данных);
- администратор информационной безопасности;
- администратор информационных систем.

Для обучения остальных категорий работников проводятся:

- внутренние семинары;
- инструктажи.

Внутренние семинары и инструктажи проводятся вышеперечисленные ответственными лицами Учреждения, а также приглашенными специалистами или другими подготовленными лицами.

Обучение каждой категории сотрудников должно проводиться не реже одного раза в год.

В Учреждении должны применяться следующие способы выявления потребностей в обучении по вопросам обеспечения информационной безопасности:

- анализ результатов контрольных мероприятий;

– анкетирование и интервьюирование руководителей подразделений и сотрудников;

– анализ специальной внешней информации (изменения внешней рыночной, правовой, технологической обстановки и т.п.);

– анализ изменений состояния человеческих ресурсов внутри Учреждения (численности персонала, перемещений сотрудников по причинам, связанным со структурными изменениями).

При выявлении потребностей также учитываются следующие положительные мотивы, влияющие на обучение сотрудников:

– стремление сотрудников к продвижению по службе;

– стремление к новым знаниям и умениям;

– стремление к уважению и признанию со стороны руководства и коллег.

Повышение осведомленности персонала по вопросам обеспечения информационной безопасности в Учреждении должно проводится на регулярной основе.

Для повышения осведомленности персонала по вопросам обеспечения информационной безопасности в Учреждении, Администратор информационной безопасности должен разрабатывать обучающие материалы.

Администратор информационной безопасности должен доводить до сотрудников Учреждения информацию о возможных угрозах информационной безопасности и их последствиях путем проведения централизованных рассылок информационных сообщений средствами электронной почты или устных инструктажей.

Администратор информационной безопасности должен на регулярной основе осуществлять мониторинг средств массовой информации (новостных лент, аналитических материалов, специализированных форумов, печатной информации и т.д.) по вопросам в области информационной безопасности.

21. Обеспечение защиты информации при выводе из эксплуатации ИС

Основаниями для вывода ИС Учреждения из эксплуатации являются:

– завершение срока эксплуатации системы, в случае если такой срок был установлен актом о вводе ИС в эксплуатацию;

– нецелесообразность эксплуатации ИС, в том числе низкая эффективность используемых технических средств и программного обеспечения, изменение правового регулирования, принятие управленческих решений, а также наличие иных изменений, препятствующих эксплуатации ИС;

– финансово-экономическая неэффективность эксплуатации ИС;

– решение руководителя Учреждения.

При наличии одного или нескольких оснований для вывода ИС из эксплуатации, формируется комиссия по выводу из эксплуатации ИС из числа работников Учреждения. В комиссию по выводу из эксплуатации ИС должны входить:

– Ответственный за организацию обработки конфиденциальной информации (или персональных данных);

– Администратор информационной безопасности;

– Администратор информационных систем.

Состав комиссии должен быть закреплен документально.

После утверждения состава, комиссия по выводу из эксплуатации, ИС готовит акт о выводе ИС из эксплуатации и передает его на утверждение руководителю Учреждения.

Акт о выводе системы из эксплуатации включает:

– основание для вывода системы из эксплуатации;

– перечень и сроки реализации мероприятий по выводу системы из эксплуатации;

– порядок, сроки, режим хранения и дальнейшего использования информационных ресурсов, включая порядок обеспечения доступа к

информационным ресурсам выводимой из эксплуатации системы и обеспечения защиты информации, содержащейся в выводимой из эксплуатации системе;

– порядок, сроки и способы информирования пользователей о выводе системы из эксплуатации.

В рамках обеспечения защиты информации в ИС Учреждения или их отдельных компонентах при выводе из эксплуатации осуществляется:

– архивирование информации, содержащейся на машинных носителях информации;

– уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации;

– работы по деинсталляции программного обеспечения ИС, программных и программно-технических средств защиты информации, демонтажу и списанию технических средств ИС (в случае если технические средства не подлежат использованию для других целей).

Объем и порядок архивирования информации определяется генеральным директором Учреждения при принятии решения о выводе из эксплуатации ИС Учреждения.

Уничтожение (стирание) информации с машинных носителей информации, выводимых из эксплуатации программно-технических средств производится администратором информационной безопасности путем перезаписи уничтожаемых (стираемых) файлов случайной битовой последовательностью, удаления записи о файлах, обнуления журнала файловой системы или полной перезаписи всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием.

Регистрацию действий по удалению защищаемой информации или уничтожению машинных носителей информации осуществляет администратор информационной безопасности с использованием Журнала учета машинных носителей информации с указанием причины удаления информации или уничтожения машинного носителя как «вывод из эксплуатации».

Ответственность за обеспечение защиты информации при выводе из эксплуатации ИС возлагается на Администратора информационной безопасности.

22. Срок действия и порядок внесения изменений

Настоящее Положение действует постоянно до своей отмены.

Плановая актуализация настоящего Положения производится не реже одного раза в год с целью приведения в соответствие определенных Положением организационных мер реальным условиям и текущим требованиям к защите информации.

Положение может быть пересмотрено внепланово в следующих случаях:

– существенные изменения информационных потоков и (или) процессов обработки информации в ИС Учреждения;

– анализ выявленных инцидентов информационной безопасности и результатов реагирования на них;

– внешние изменения (например, изменения нормативных правовых документов в области защиты информации, социальные или политические изменения);

– идентификация новых или изменившихся угроз и(или) уязвимостей.

Ответственность за актуализацию Положения (плановую и внеплановую) несет Администратор информационной безопасности.

23. Ответственность

Ответственность за соблюдение требований настоящего Положения возлагается на всех сотрудников Учреждения, на которых распространяется это Положение.

Лица, виновные в нарушении настоящего Положения и требований законодательства в области информационной безопасности, несут дисциплинарную, гражданскую, административную, уголовную и иную предусмотренную законодательством Российской Федерации ответственность.

Ответственность за осуществление общего контроля выполнения требований Политики несет Ответственный за организацию обработки конфиденциальной информации (или персональных данных) и Администратор информационной безопасности.

Приложение № 1

Заявка на установку программного обеспечения АРМ

Заявка

Кому: Администратору информационной безопасности

От кого: От (должность, ФИО)

Дата: «___» _____ 20___ г.

Тема: О согласовании установки ПО

Прошу Вас произвести установку/удаление/модификацию следующего программного обеспечения:

_____
_____
_____
_____
_____

в связи с необходимостью решения следующих задач:

_____
_____
_____
_____
_____
_____

_____
(должность, подпись, расшифровка подписи, дата)

Согласовано

_____
(должность, подпись, расшифровка подписи, дата)

Приложение № 2

Журнал регистраций дополнений ПО

Журнал регистраций дополнений программного обеспечения

период действия с « »_____ 20__ года по « » _____ 20__ года

№ п/п	– Дата внесения изменений	- Инвентарный номер АРМ	– Владелец АРМ/отдел	– Описание изменений (наименование и версия ПО)
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–
–	–	–	–	–

Приложение № 3

Ответственному за организацию
обработки конфиденциальной
информации М. Х. Чанкаев

(резолюция)

ЗАЯВКА

на внесение изменений в списки пользователей
информационной системы _____
_____
_____

и наделение пользователя полномочиями доступа к информационной системе

Прошу зарегистрировать пользователя (исключить из списка пользователей,
(ненужное зачеркнуть)
изменить полномочия пользователя) _____
_____
(должность с указанием структурного подразделения)
_____
(фамилия имя и отчество работника)

предоставив ему полномочия, необходимые (исключив ему полномочия, необходимые)
(ненужное зачеркнуть)
для решения задач: _____
_____
_____

Руководитель _____
(наименование заказывающего структурного подразделения)

«___» _____ 20___ г. _____ _____
(подпись) (фамилия)

ЗАДАНИЕ

на внесение изменений в списки пользователей информационной системы

Администратору информационной безопасности

_____
(фамилия и инициалы исполнителя)

Произвести изменения в списках пользователей указанной информационной системы

Ответственный за организацию обработки конфиденциальной информации

«___» _____ 20___ г.

Приложение № 4

ЖУРНАЛ
РЕГИСТРАЦИИ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

п/п	ФИО, должность, структурное подразделение сотрудника обнаружившего инцидент	Дата выявления инцидента	Описание инцидента	Принятые меры по устранению последствий инцидента	Причины возникновения инцидента	Размер потенциально-возможного ущерба	Размер фактического ущерба	Принятые меры по предотвращению повторного возникновения инцидента
	2	3	4	5	6	7	8	9

Приложение № 5

ЖУРНАЛ УЧЕТА ИЗМЕНЕНИЙ В КОНФИГУРАЦИИ ИС

Журнал начат: [дата]

[Должность] [ФИО] [Подпись]

Журнал завершен: [дата]

[Должность] [ФИО] [Подпись]

№ п/п	Дата и время внесения изменения	Цель проведения изменения	Отчет об проведения изменения	Компоненты, затронутые изменением	ФИО лица, проводившего изменение	Подпись лица, проводившего изменение	ФИО администратора информационной безопасности	Подпись администратора информационной безопасности
1	2	3	4	5	6	7	8	9

Приложение № 6

ЖУРНАЛ УЧЕТА НЕШТАТНЫХ СИТУАЦИЙ

Журнал начат: [дата]

[Должность] [ФИО] [Подпись]

Журнал завершен: [дата]

[Должность] [ФИО] [Подпись]

№ п/п	Дата, ИС, техническое средство, описание ситуации, проделанные работы	Подпись исполнителя	Подпись администратора информационной безопасности
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			

Приложение № 7

ЖУРНАЛ УЧЕТА МЕРОПРИЯТИЙ ПО КОНТРОЛЮ ЗАЩИЩЕННОСТИ ИС

Журнал начат: [дата]

[Должность] [ФИО] [Подпись]

Журнал завершен: [дата]

[Должность] [ФИО] [Подпись]

№ п/п	Дата проведения мероприятия	Плановое /внеплановое проведение	Выявленные несоответствия	Рекомендации по устранению несоответствий	ФИО администратора информационной безопасности	Подпись администратора информационной безопасности
1	2	3	4	5	6	7

Приложение № 8

ЖУРНАЛ УЧЕТА МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

Журнал начат: [дата]

[Должность] [ФИО] [Подпись]

Журнал завершен: [дата]

[Должность] [ФИО] [Подпись]

№ п/п	Регистра-ционный номер	Дата учета	Тип / емкость носителя	Серийный номер	Отметка о постановке на учет (ФИО, подпись, дата)	Отметка о снятии с учета (ФИО, подпись, дата)	Местоположение носителя	Сведения об уничтожении носителя / стирании информации
1	2	3	4	5	6	7	8	9

Приложение № 9

ШТАМП

АРМ Инв. №_____

Размещение _____

Ответственный (-ая) _____

РАЗРЕШЕНО ОБРАБАТЫВАТЬ КИ (в т.ч. ПДн)

НЖМД № _____

_____

М.П.

Приложение № 10

ЛИЦЕВОЙ СЧЕТ

на передачу защищаемого носителя конфиденциальной информации

Тип: _____

Производитель: _____

Модель: _____

Серийный номер: _____

№ п/п	Отметка о получении носителя			Категория информации на носителе	Отметка в обратном приеме		
	Дата	ФИО	Подпись		Дата	ФИО	Подпись

Приложение № 11

ЖУРНАЛ РЕЗЕРВИРОВАНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Журнал начат: [дата]

[Должность] [ФИО] [Подпись]

Журнал завершен: [дата]

[Должность] [ФИО] [Подпись]

№ п/п	Резервируемый ресурс	Вид резервирования (восстановления)	Носитель резервных копий	Ответственный (должность, ФИО, подпись)	Дата резервирования	Примечания
1	2	3	4	5	6	7