СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Администратор (системный, безопасности)	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) информационной системы (администратор системный) и (или) ее системы защиты персональных данных (администратор безопасности) в соответствии с установленной ролью
Аутентификация	Проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе)
Безопасность персональных данных	Состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных
Вирус (компьютерный, программный)	Исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению
Внешняя информационная система	Информационная система, взаимодействующая с информационной системой оператора из-за пределов границ информационной системы оператора
Внешняя информационно-телекоммуникационная сеть	Информационно-телекоммуникационная сеть, взаимодействующая с информационной системой оператора из-за пределов границ информационной системы
Вредоносная программа	Программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы
Доступ к информации	Возможность получения информации и ее использования
Доступность	Свойство безопасности информации, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовать
Защищаемая информация	Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми

	собственником информации
Защищенные линии связи	Линии (каналы) связи, при передаче информации по которым обеспечивается требуемый уровень ее защищенности (конфиденциальность, целостность и (или) доступность)
Идентификатор	Представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной системе
Идентификация	Присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Информация ограниченного доступа	Информация, доступ к которой ограничен федеральными законами
Информационные технологии	Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов
Инцидент	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)
Исходная ключевая информация	Совокупность данных, предназначенных для выработки по определенным правилам криптоключей
Ключевая информация	Специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока
Ключевой документ	Физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию
Ключевой носитель	Физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации)

Компрометация	Хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам
Компонент программного обеспечения	Составная часть (программный модуль) программного обеспечения, выполняющая определенную функцию
Контролируемая зона	Пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств
Конфиденциальность персональных данных	Обязательное для выполнения лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания
Криптографический ключ (криптоключ)	Совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе
Модель угроз	Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации
Нарушитель безопасности информации	Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационной системе
Недекларированные возможности	Функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации
Несанкционированный доступ	Доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами
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
Отказ в обслуживании	Препятствие санкционированному доступу к ресурсам информационной системы или задержка операций и функций информационной системы
Периметр информационной системы	Физическая и (или) логическая граница информационной системы, в пределах которой обеспечивается защита информации в соответствии с едиными правилами и процедурами, а также контроль за реализованными мерами защиты информации
Персональных данных	Любая информация, относящаяся к прямо или косвенно определённому, или определяемому физическому лицу (субъекту персональных данных)
Персональный компьютер (ПК)	Вычислительная машина, предназначенная для эксплуатации пользователем Учреждения в рамках исполнения должностных обязанностей
Пользователь информационной системы	Лицо, участвующее в функционировании информационной системы или использующее результаты её функционирования
Пользователи СКЗИ	Работники Учреждения, непосредственно допущенные к работе с СКЗИ
Правила разграничения доступа	Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа
Ресурс информационной системы	Именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы
Роль	Предопределенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и информационной системой
Событие безопасности (информационной)	Идентифицированное возникновение состояния информационной системы (сегмента, компонента информационной системы), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации

Средство криптографической защиты информации (СКЗИ)	Совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.
Средства вычислительной техники	Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем
Субъект доступа	Пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа
Технические средства	Средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации
Управление доступом	Ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа
Целостность информации	Свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение субъектами доступа, имеющими на него право

СПИСОК ПРИНЯТЫХ СОКРАЩЕНИЙ

АРМ	Автоматизированное рабочее место
ВП	Вредоносная программа
ЕИС ПГиМУ СО	Единая информационная система для предоставления государственных и муниципальных услуг в сфере образования
ИС	Информационная система персональных данных
НЖМД	Накопитель на жестком магнитном диске
НСД	Несанкционированный доступ к информации
ОС	Операционная система
ОТСС	Основные технические средства и системы
ПДн	Персональные данные
ПО	Программное обеспечение
ПЭВМ	Персональная электронно-вычислительная машина
СЗИ	Средство защиты информации
СЗПДн	Система защиты персональных данных
СКЗИ	Средство криптографической защиты информации
ТС	Технические средства
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящие Правила определяют порядок работы персонала на Автоматизированном рабочем месте оператора государственной информационной системы «Единая информационная система для предоставления государственных и муниципальных услуг в сфере образования» (ИС) в части обеспечения защиты информации, в т.ч. обеспечения безопасности персональных данных (ПДн), порядок использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты, порядок допуска работников и посторонних лиц помещение, в котором расположены технические средства ИС.

Действие настоящих Правил распространяется на вопросы, связанные с обработкой защищаемой информации, в т.ч. ПДн, в ИС, осуществляемой с использованием средств автоматизации.

Настоящие Правила разработаны на основании следующих основных нормативных правовых актов и документов в области обеспечения защиты информации, в т.ч. обеспечения безопасности персональных данных:

- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Федеральных закон от 27.07.2006 г. № 149 «Об информации, информационных технологиях и о защите информации»;
- постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2 ОСНОВНЫЕ ТРЕБОВАНИЯ

2.1 Обеспечение безопасности ПДн при их обработке в ИС достигается применением организационных и технических мер, причем в интересах обеспечения безопасности в обязательном порядке подлежат защите технические и программные средства, используемые при обработке ПДн, и носители информации.

2.2 Основными мерами защиты информации (ПДн) являются:

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам (ИР) ИС и связанным с ее использованием работам, документам;
- ограничение доступа пользователей в помещения, где размещены технические средства (ТС) ИС, позволяющие осуществлять обработку ПДн, а также хранятся носители информации;
- разграничение доступа пользователей и обслуживающего персонала к ИР, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа (НСД) и действий пользователей, обслуживающего персонала и посторонних лиц;
- учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;
- резервирование ТС, дублирование массивов и носителей информации;
- использование СЗИ, прошедших в установленном порядке процедуру оценки

соответствия требованиям безопасности информации;

– использование защищенных каналов связи;

– размещение ТС, позволяющих осуществлять обработку ПДн в пределах охраняемой территории;

– размещение дисплеев и других средств отображения информации, исключающее ее несанкционированный просмотр;

– организация физической защиты помещений и собственно ТС, позволяющих осуществлять обработку ПДн;

– предотвращение внедрения в ИС вредоносных программ (программ-вирусов) и программных закладок.

2.3 Все применяемые средства защиты информации должны учитываться в Журнале учета СЗИ. Форма Журнала приведена в Приложении 1. Организация ведения Журнала учета СЗИ возлагается на Администратора безопасности.

3 ПОРЯДОК ДОПУСКА ПОЛЬЗОВАТЕЛЕЙ К РАБОТЕ НА АРМ

Разрешительная система доступа представляет собой совокупность процедур оформления прав субъектов на доступ к информационным ресурсам (ИР) (объектам доступа) ИС, а также прав и обязанностей ответственных лиц, осуществляющих реализацию этих процедур.

Подлежащие защите информационные ресурсы включаются в «Перечень информационных ресурсов, подлежащих защите на АРМ оператора ЕИС ПГиМУ СО», утверждаемый руководителем Учреждения;

Объектами доступа являются:

– информационные ресурсы ИС.

Субъектами доступа являются:

– уполномоченные сотрудники образовательной организации.

Субъекты доступа несут персональную ответственность за соблюдение ими установленного на объекте информатизации порядка обеспечения защиты информационных ресурсов.

Ответственным лицом, осуществляющим реализацию процедур оформления прав субъектов на доступ к информационным ресурсам ИС, является Администратор безопасности.

Первоначальный допуск пользователей к работе в ИС осуществляется на основании «Перечня лиц, доступ которых к защищаемой информации, в т.ч. персональным данным, обрабатываемым на АРМ оператора ЕИС ПГиМУ СО» утвержденного приказом руководителя Учреждения.

Для обеспечения персональной ответственности за свои действия каждому пользователю ИС, допущенному к работе с защищаемой информацией, присваивается имя (учетная запись пользователя), под которым он регистрируется и осуществляет работу в системе. В случае производственной необходимости пользователю ИС могут быть сопоставлены несколько уникальных имен (учетных записей). В случае использования несколькими работниками при работе в ИС одного и того же имени пользователя ("группового имени"), вход/выход в ИС указанием времени работы на АРМ должен фиксироваться в «Журнале учета рабочего времени на АРМ оператора ЕИС ПГиМУ СО» (Приложение 2).

При регистрации и назначении прав доступа пользователей в ИС должны выполняться следующие требования:

- учетные записи всех пользователей привязываются к конкретным автоматизированным рабочим местам (АРМ), за исключением учетных записей технического персонала, обслуживающего компоненты ИС;

- при регистрации пользователей проводится проверка соответствия уровня доступа

возложенным на пользователя задачам (вмененным обязанностям);

- назначенные пользователю права доступа документируются;
- пользователь знакомится под роспись с предоставленными ему правами доступа и порядком его осуществления;
- в ИС предусматривается разрешение доступа к сервисам только аутентифицированным пользователям;
- при внесении нового пользователя разрабатывается и обновляется формальный список всех пользователей, зарегистрированных для работы в ИС;
- при изменении должностных обязанностей (увольнении) пользователя проводится немедленное исправление (аннулирование) прав его доступа;
- Администратором безопасности проводится удаление всех неиспользуемых учетных записей. Предусмотренные в системе запасные идентификаторы недоступны другим пользователям.

Процедура регистрации (создания учетной записи) пользователя и предоставления (или изменения) ему прав доступа к ресурсам ИС осуществляется с использованием сертифицированных средств защиты информации от несанкционированного доступа.

Для загрузки компьютера в ИС предусмотрены два типа учетных записей:

- учетная запись администратора безопасности позволяет производить настройку средств защиты информации и добавлять/удалять пользователей в систему, производить установку и настройку программного обеспечения на АРМ ИС;
- учетная запись пользователя наделена ограниченными правами.

После определения роли пользователя и в соответствии с обозначенными для него в Матрице доступа (Приложение 3) правами Администратор безопасности в соответствии с документацией на средства защиты производит необходимые действия по созданию (изменению, удалению) учетной записи пользователя, присвоению ему начального значения пароля и заявленных прав доступа к ресурсам ИС, включению его в соответствующие группы пользователей и другие необходимые действия.

После создания учетной записи, пользователь должен авторизоваться в системе.

Администратор безопасности обязан проверить наличие записей о входе пользователя в систему в журнале регистрации событий средств зашиты информации от несанкционированного доступа.

Для всех пользователей ИС устанавливается режим принудительного запроса смены пароля не реже одного раза в 90 дней, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки - 5 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации - 15 минут.

В случае производственной необходимости пользователю ИС могут быть сопоставлены несколько уникальных имен (учетных записей).

При изменении должностных обязанностей сотрудника, связанных с переводом в другое подразделение, переводом на другую должность и т.п., учетная запись пользователя подлежит изменению (корректировке), при этом старые полномочия аннулируются.

После внесения изменений в Матрицу доступа Администратор безопасности производит настройку средств защиты рабочих станций (автоматизированных рабочих мест).

На время отпуска пользователей Администратором безопасности осуществляется блокирование их учетных записей.

Контроль выполнения требований разрешительной системы доступа к защищаемой информации (ПДн) возлагается на Администратора безопасности.

3.1 Допуск к информационным ресурсам сторонних организаций, деятельность которых не связана с исполнением функций Учреждения

К организациям, деятельность которых не связана с исполнением функций Учреждения, могут относиться:

- правоохранительные органы;
- судебные органы;
- органы статистики;
- органы исполнительной и законодательной власти субъектов Российской Федерации;
- средства массовой информации и пр.

Допуск к информационным ресурсам сторонних организаций, деятельность которых не связана с исполнением функций Учреждения, регламентируется законодательством Российской Федерации, договорами и соглашениями об информационном обмене и другими нормативными актами.

3.2 Допуск к информационным ресурсам ИС сторонних организаций, выполняющих работы в Учреждении на договорной основе

К организациям, выполняющим работы на договорной основе, могут относиться:

- организации, осуществляющие монтаж и настройку технических средств ИС, сопровождение прикладного программного обеспечения;
- организации, оказывающие услуги в области защиты информации (проведение специальных проверок и исследований, монтаж и настройка средств защиты информации, контроль эффективности системы защиты информации, аттестация объектов информатизации и т.п.);
- организации, осуществляющие поставку товаров для обеспечения повседневной деятельности (мебели, канцтоваров, оргтехники, расходных материалов и т.п.).

Порядок допуска определяется в договоре на выполнение работ (оказание услуг). Кроме того, лицам, привлекаемым на договорной основе для обеспечения функционирования информационной системы (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами оператора, на срок действия договора, должны быть присвоены учетные записи.

Решением о допуске является подписанный в установленном порядке договор на выполнение работ или оказание услуг.

В договор на оказание услуг включается условие о неразглашении сведений, содержащих персональные данные, а также служебной информации, ставшей известной в ходе выполнения работ, если для их выполнения предусмотрено использование таких сведений. Со всех работников сторонней организации, участвующих в выполнении работ, в этом случае берется подписка о неразглашении таких сведений.

3.3 Контроль функционирования разрешительной системы допуска к информационным ресурсам организации

Контроль функционирования разрешительной системы допуска к информационным ресурсам организуется в соответствии с:

- планом основных мероприятий по защите информации на текущий год;
- функциональными обязанностями должностных лиц;
- приказами руководителя Учреждения.

Контроль функционирования разрешительной системы допуска к информационным ресурсам ИС осуществляется ответственными лицами. Организация контроля возлагается на Администратора безопасности.

4 ПОРЯДОК ДОПУСКА СОТРУДНИКОВ И ИНЫХ ЛИЦ В ПОМЕЩЕНИЯ С ЭЛЕМЕНТАМИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

4.1 Требования к помещениям, в которых расположены элементы ИС

Бесконтрольный доступ посторонних лиц в помещения с элементами ИС должен быть исключён.

Для защиты помещений, в которых расположены технические средства ИС, должны приниматься меры для минимизации воздействий огня, дыма, воды, пыли, взрыва, химических веществ, а также кражи.

4.2 Доступ в помещения, которых расположены элементы ИС

Должен быть определен список помещений, предназначенных для обработки ПДн средствами ИС, и организован контроль доступа служащих и посетителей в помещения, в которых установлены технические средства (далее - ТС) ИС и осуществляется обработка ПДн, а также хранятся машинные носители информации (ПДн).

Доступ сотрудников структурных подразделений в помещения, в которых осуществляется обработка ПДн, организовывается на основании утвержденного руководителем «Перечня лиц, имеющих право доступа в помещения, в которых расположены технические средства ИС».

Доступ посторонних лиц в помещения с элементами ИС, должен осуществляется только ввиду служебной необходимости и в сопровождении ответственных лиц.

На момент присутствия посторонних лиц в помещении ИС, должны быть приняты меры по недопущению ознакомления посторонних лиц с ПДн (например: мониторы повёрнуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке или накрыты чистыми листами бумаги).

По окончании рабочего дня помещения с элементами ИС должны сдаваться под охрану. При этом все окна и двери в смежные помещения должны быть надёжно закрыты, материальные носители ПДн должны быть убраны в запираемые шкафы (сейфы), АРМ выключены или заблокированы.

В нерабочее время доступ сотрудников Учреждения, представленных в «Перечне лиц, имеющих право доступа в помещения, в которых расположены технические средства ИС», и иных лиц в помещения с установленными техническими средствами ИС осуществляется с разрешения Администратора безопасности.

4.3 Требования к помещениям, в которых установлены СКЗИ, или хранятся ключевые документы к ним

Помещения, в которых установлены СКЗИ, или хранятся документы к ним, должны быть оснащены входными дверьми с замками.

В ИС должно обеспечиваться постоянное закрытие дверей помещений с элементами СКЗИ на замок и их открытие только для санкционированного прохода, а также опечатывание помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

Для хранения ключевых документов, эксплуатационной и технической документации на СКЗИ, инсталлирующих носителей должно быть предусмотрено необходимое число надёжных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Ключи от хранилища должны находиться у ответственного пользователя криптосредств (Ответственного за обеспечение функционирования и безопасности криптосредств).

По окончании рабочего дня помещения, в которых расположены СКЗИ, и хранятся ключевые документы к ним, и установленные в нем хранилища должны быть закрыты, хранилища опечатаны.

В обычных условиях помещения, находящиеся в них опечатанные хранилища, могут быть вскрыты только пользователями криптосредств или ответственным пользователем криптосредств. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному пользователю криптосредств. Прибывший ответственный пользователь криптосредств должен оценить возможность компрометации хранящихся ключевых и других документов и принять, при необходимости, меры к локализации последствий компрометации персональных данных и к замене скомпрометированных криптоключей.

Размещение и монтаж криптосредств, а также другого оборудования, функционирующего с криптосредствами, в помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

5 АДМИНИСТРАТОР БЕЗОПАСНОСТИ

5.1 Общие положения

Администратор безопасности назначается приказом руководителя Учреждения.

Администратор безопасности в своей работе руководствуется настоящими Правилами, требованиями законов и иных нормативно-правовых актов Российской Федерации по вопросам защиты персональных данных, руководящими и нормативными документами ФСТЭК России, ФСБ России и внутренними организационно-распорядительными документами Учреждения.

Администратор безопасности является ответственным должностным лицом Учреждения, уполномоченным на проведение работ по обеспечению устойчивого функционирования элементов ИС, технической защите информации и поддержанию достигнутого уровня защиты ИС и ее ресурсов на этапах промышленной эксплуатации и модернизации.

Администратор безопасности осуществляет методическое руководство пользователей ИС, в вопросах обеспечения безопасности персональных данных.

Требования Администратора безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИС.

Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИС, состояние и поддержание установленного уровня защиты ИС.

В распоряжении Администратора безопасности должен быть личный сейф, железный шкаф или др.

На время отсутствия Администратора безопасности (отпуск, болезнь, пр.) его обязанности исполняет лицо, назначенное в установленном порядке, которое приобретает соответствующие права и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

5.2 Задачи администратора безопасности

Основными задачами Администратора безопасности являются:

- обеспечение устойчивого функционирования и работоспособности элементов ИС, в т.ч. АРМ пользователей;
- поддержание необходимого уровня защиты ИС от несанкционированного доступа (далее - НСД) к информации;
- установка средств защиты информации на элементах ИС и контроль выполнения правил их эксплуатации;
- сопровождение СЗИ, используемых в ИС;

– периодическое обновление используемых СЗИ (при необходимости);

– проведение комплекса мероприятий по предотвращению инцидентов ИБ;

– оперативное реагирование на нарушения требований по ИБ ИС и участие в их прекращении.

В рамках выполнения основных задач Администратор безопасности осуществляет:

– обеспечение установки, настройки и своевременного обновления элементов ИС:

программного обеспечения автоматизированных рабочих мест (АРМ) пользователей (операционные системы, прикладное и специальное программное обеспечение (ПО);

аппаратных средств;

коммутационного оборудования.

– текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств СЗИ;

– принятие мер по своевременному восстановлению и выявлению причин в случае отказа работоспособности технических средств и программного обеспечения элементов ИС;

– текущий контроль технологического процесса автоматизированной обработки информации;

– текущий контроль неизменности состояния СЗИ их параметров и режимов защиты;

– текущий контроль физической сохранности средств и оборудования ИС;

– контроль исполнения пользователями установленных в ИС правил организации парольной защиты;

– анализ журналов учета событий безопасности СЗИ, с целью выявления возможных нарушений;

– учет машинных носителей информации, используемых в ИС;

– контроль действий пользователей при работе с машинными носителями информации;

– ввод полномочий пользователей в разрешительную систему доступа (матрицу доступа) и их своевременную корректировку;

– контроль за соблюдением пользователями установленных в ИС правил по организации антивирусного контроля;

– участие в проведении служебных расследований фактов нарушений или угрозы нарушений безопасности информации;

– контроль соблюдения нормативных требований по защите информации, обеспечения комплексного использования технических средств, методов и организационных мероприятий по безопасности информации пользователями ИС;

– методическую помощь пользователям ИС по вопросам обеспечения защиты информации и работы с используемыми СЗИ.

5.3 Обязанности администратора безопасности информации

Администратор безопасности обязан:

– знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководств по защите информации и распоряжений, регламентирующих порядок действий по защите информации;

– осуществлять установку, настройку и сопровождение программного обеспечения АРМ пользователей (системного, прикладного и специального программного обеспечения) и СЗИ, используемых в ИС;

– обеспечивать работоспособность технических средств обработки информации в ИС;

– участвовать в контрольных и тестовых испытаниях и проверках элементов ИС;

– участвовать в приемке новых программных средств обработки информации в

ИС;

– обеспечивать доступ к защищаемой информации пользователям ИС согласно их правам доступа при получении оформленного соответствующим образом разрешения (заявки);

– уточнять в установленном порядке обязанности пользователей ИС при обработке защищаемой информации;

– осуществлять резервное копирования объектов защиты в ИС;

– анализировать состояние защиты ИС;

– контролировать правильность функционирования средств защиты информации и неизменность их настроек;

– контролировать физическую сохранность технических средств обработки информации;

– контролировать исполнение пользователями ИС введенного режима безопасности, а также правильность работы с элементами ИС и средствами защиты информации;

– контролировать исполнение пользователями правил парольной политики;

– еженедельно анализировать журналы учета событий безопасности, регистрируемых средствами защиты, с целью контроля действий пользователей и выявления возможных нарушений;

– осуществлять при необходимости установку обновлений программного обеспечения, в т.ч. программного обеспечения средств защиты информации, а также контроль такой установки в случае выполнения данного вида работ сотрудниками сторонних организаций;

– не допускать установку, использование, хранение и размножение в ИС программных средств, не связанных с выполнением функциональных задач;

– вести контроль за соблюдением установленного в ИС порядка организации работы с машинными носителями информации;

– не допускать к работе на элементах ИС посторонних лиц;

– осуществлять периодические контрольные проверки автоматизированных рабочих мест пользователей ИС;

– оказывать помощь пользователям ИС в части применения средств защиты и консультировать по вопросам введенного режима защиты;

– в случае необходимости информировать руководство о состоянии защиты ИС и о нештатных ситуациях и допущенных пользователями нарушениях установленных требований по защите информации;

– в случае отказа работоспособности СЗИ в ИС принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;

– предпринимать необходимые меры при выявлении уязвимостей в рамках своих должностных обязанностей. В качестве источников информации об уязвимостях могут использоваться опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей. В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты информации, изменение режима и порядка использования системы), направленные на устранение возможности использования выявленных уязвимостей;

– в случае выявления нарушений режима безопасности информации, а также возникновения нештатных и аварийных ситуаций принимать необходимые меры с целью

ликвидации их последствий;

– обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки информации, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта не рекомендуется передавать ремонтным организациям узлы и блоки с элементами накопления и хранения. информации.

5.4 Права администратора безопасности

Администратор безопасности имеет право:

– отключать от ресурсов ИС пользователей, осуществивших НСД к защищаемым ресурсам ИС или нарушивших другие требования по ИБ;

– в установленном порядке изменять конфигурацию элементов ИС;

– требовать от пользователей и администраторов ИС безусловного соблюдения установленной технологии обработки информации и выполнения требований локальных документов, регламентирующих вопросы обеспечения защиты информации;

– давать пользователям обязательные для исполнения указания и рекомендации по вопросам ИБ;

– инициировать проведение служебных расследований по фактам нарушений установленных требований обеспечения ИБ, НСД, утраты, порчи защищаемой информации и технических средств ИС;

– осуществлять взаимодействие с руководством Учреждения и персоналом ИС по вопросам обеспечения безопасности информации;

– запрещать устанавливать на автоматизированных рабочих местах нештатное программное и аппаратное обеспечение;

– запрашивать и получать от начальников и специалистов структурных подразделений Учреждения информацию и материалы, необходимые для организации своей работы;

– вносить на рассмотрение руководства предложения по улучшению состояния защиты информации в ИС;

– действовать в обход установленных процедур идентификации и аутентификации только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств);

– принимать участие в проведении мероприятий по контролю за обеспечением безопасности информации в ИС.

5.5 Действия администратора безопасности при обнаружении попыток НСД

К попыткам НСД относятся:

– сеансы работы с информационными ресурсами ИС незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят операции доступа к определенным данным или манипулирования ими;

– действия третьего лица, пытающегося получить доступ (или получившего доступ) к информационным ресурсам ИС с использованием учетной записи администратора или другого пользователя ИС, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

При выявлении факта/попытки НСД Администратор безопасности обязан:

– прекратить доступ к информационным ресурсам со стороны выявленного участка НСД;

– доложить в случае необходимости руководителю Учреждения о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;

– известить начальника структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;

– проанализировать характер НСД;

– по решению руководства осуществить действия по выяснению причин, приведших к НСД;

– предпринять меры по предотвращению подобных инцидентов в дальнейшем.

5.6 Ответственность администратора безопасности

Администраторы безопасности, виновные в несоблюдении настоящей Инструкции, расцениваются как нарушители законодательства Российской Федерации в области защиты информации и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

6 ОРГАНИЗАЦИЯ РАБОТЫ ПОЛЬЗОВАТЕЛЯ НА АРМ

6.1 Общие положения

Пользователем информационной системы является каждый сотрудник Учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации, в т.ч. персональных данных, и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты информации ИС.

Пользователь несет персональную ответственность за свои действия.

Пользователь в своей работе руководствуется настоящими Правилами, нормативными документами ФСТЭК России, ФСБ России, внутренними регламентирующими документами Учреждения и другими документами.

Методическое руководство работой пользователя в части выполнения положений законодательства Российской Федерации и внутренних документов Учреждения в области защиты информации осуществляется Администратором безопасности ИС.

6.2 Должностные обязанности

Пользователь ИС, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИС, несет персональную ответственность за свои действия и обязан:

– решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИС, присвоенными Администратором безопасности данному пользователю. При этом для хранения файлов, содержащих конфиденциальные сведения, разрешается использовать только соответствующим образом учтенные машинные носители информации;

– знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации;

– экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами. Шторы на оконных проемах должны быть завешаны (жалюзи закрыты);

– знать и строго выполнять правила работы со средствами защиты информации, установленными на вверенном ему автоматизированном рабочем месте;

– соблюдать требования Инструкции по организации парольной защиты;

– в случае отказа системы в идентификации пользователя, либо не подтверждения личного пароля немедленно обратиться к Администратору безопасности.

– строго соблюдать установленные требования по организации антивирусной защиты. В случае обнаружения вирусов немедленно сообщить об этом Администратору безопасности;

– знать и соблюдать установленные требования по учету, хранению машинных носителей информации;

– немедленно ставить в известность Администратора безопасности и в случае подозрения, а также при обнаружении фактов совершения попыток несанкционированного доступа к ресурсам ИС: несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИС, отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ИС, выхода из строя или неустойчивого функционирования узлов ИС или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, непредусмотренных отводов кабелей и подключенных устройств;

– для получения консультаций по вопросам работы ПЭВМ и настройке программного обеспечения необходимо обращаться к и работы средств защиты информации обращаться к Администратору безопасности;

– принимать меры по реагированию, в случае возникновения нештатных и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций;

– проходить периодическую проверку знаний положений нормативной документации по вопросам защиты информации в ходе периодического контроля соблюдения режима безопасности информации в ИС.

Пользователям **ЗАПРЕЩАЕТСЯ**:

– использовать компоненты программного и аппаратного обеспечения ИС в неслужебных целях;

– отключать (блокировать) средства защиты информации;

– самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИС или устанавливать дополнительно любые программные и аппаратные средства;

– осуществлять обработку защищаемой информации в присутствии посторонних (не допущенных к данной информации) лиц;

– сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИС;

– записывать и хранить защищаемую информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации;

– оставлять включенной без присмотра рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры). При этом, на устройстве отображения (мониторе) после блокировки сеанса не должна отображаться информация сеанса пользователя (в том числе использование «хранителя экрана», гашение экрана или иные способы);

– оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок ставить в известность Администратора безопасности;

– осуществлять какие-либо действия в ИС до прохождения процедур идентификации и аутентификации;

– подключать к рабочей станции и вычислительной сети личные внешние носители и мобильные устройства;

– отключать (блокировать) средства защиты информации;

– привлекать посторонних лиц для производства ремонта или настройки АРМ;

– разглашать защищаемую информацию третьим лицам;

– самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

7.3 Права и ответственность пользователей

Пользователь ИС имеет право в отведенное ему время решать поставленные задачи в соответствии с его полномочиями к ресурсам ИС и вверенным ему техническим и программным средствам.

Пользователь ИС, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИС, несет персональную ответственность за свои действия.

Пользователь ИС несет ответственность по действующему законодательству за разглашение сведений конфиденциального характера, ставших известными ему по роду работы.

7 ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

7.1 Требования к организации парольной защиты

Личные пароли должны генерироваться и распределяться централизованно Администратором безопасности либо выбираться пользователями ИС самостоятельно.

В случае формирования личных паролей пользователей централизованно, ответственность за правильность их формирования и распределения возлагается на Администратора безопасности ИС.

Полная плановая смена паролей в ИС проводится не реже одного раза в 90 дней.

Внеплановая смена личного пароля пользователя или удаление учетной записи в случае прекращения его полномочий (увольнение, переход на другую должность в ИС и т.п.) должна производиться Администратором безопасности немедленно после окончания последнего сеанса работы пользователя в ИС.

В ИС устанавливается ограничение на количество неуспешных попыток аутентификации (ввода логина и пароля) пользователя, равное 5, после чего учетная запись блокируется на период времени от 3 до 15 минут.

Разблокирование учетной записи осуществляется Администратором безопасности.

После 15 минут бездействия (неактивности) пользователя в ИС происходит автоматическое блокирование сеанса доступа в АРМ и ИС соответственно.

В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых пользователей в их отсутствие, такие пользователи обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте передавать на хранение Администратору безопасности информации. Запечатанные конверты с паролями пользователей должны храниться в сейфе у Администратора безопасности.

В случае утечки информации о зарегистрированном пользователе необходимо немедленно удалить данные об этом пользователе и зарегистрировать заново его с новым идентификатором.

Внеплановая смена личного пароля или удаление учетной записи пользователя, в случае прекращения его полномочий (увольнение, переход на другую работу, в другое подразделение организации и т.п.), должны немедленно производиться Администратором безопасности после окончания последнего сеанса работы данного пользователя в ИС.

Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) Администратора безопасности.

В случае компрометации личного пароля пользователя должны быть немедленно предприняты меры в соответствии с п.2.10 или п.2.11 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

Хранение пользователем зарегистрированных идентификаторов и значений своих паролей на бумажном носителе допускается только в сейфе у Администратора безопасности информации.

Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на Администратора безопасности.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

7.2 Требования к формированию паролей

Пользователи и Администратор безопасности ИС при формировании паролей должны руководствоваться следующими требованиями:

Длина пароля должна быть не менее 6 символов.

В пароле должны обязательно присутствовать символы из следующих:

- буквы в верхнем регистре;
- буквы в нижнем регистре;
- цифры;
- специальные символы, не принадлежащие алфавитно-цифровому набору (например: !, @, #, $, &, *, % и т.п.).

Пароль не должен включать в себя легко вычисляемые сочетания символов (например, «112», «911» и т.п.), а также общепринятые сокращения (например, «ЭВМ», «ЛВС», «USER» и т.п.).

Пароль не должен содержать имя учетной записи пользователя или наименование его АРМ, а также какую-либо его часть.

Пароль не должен основываться на именах и датах рождения пользователя или его родственников, кличек домашних животных, номеров автомобилей, телефонов и т.д., которые можно угадать, основываясь на информации о пользователе.

Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например, «1111111», «wwwww» и т.п.).

Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, «1234567», «qwerty» и т.п.).

При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

7.3 Правила ввода паролей

Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и пр.).

В случае блокировки учетной записи пользователя после превышения попыток ввода данных аутентификации (логина и пароля) в ИС, Пользователю необходимо уведомить

Администратора безопасности для проведения процедуры разблокировки его учетной записи.

8 ОРГАНИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ

Организация антивирусной защиты в ИС, а также контроль над работой пользователей по применению на автоматизированных рабочих местах ИС средств антивирусной защиты осуществляется Администратором безопасности.

Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящих Правил осуществляется Администратором безопасности.

8.1 Организация антивирусного контроля в ИС

К использованию в ИС допускаются только лицензионные и сертифицированные ФСТЭК России антивирусные средства, закупленные у разработчиков (поставщиков) указанных средств.

Установка и настройка средств антивирусного контроля, а также обновление антивирусных баз в ИС, осуществляется Администратором безопасности в соответствии с руководствами по применению конкретных антивирусных средств.

Контроль целостности и антивирусный контроль всех дисков и файлов элементов ИС, должен проводиться регулярно (но не реже 1 раза в неделю) в автоматическом режиме в соответствии с установленным расписанием.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), Администратором безопасности должна быть выполнена антивирусная проверка.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь обязан поставить в известность Администратора безопасности ИС, который обязан в таком случае провести внеочередной антивирусный контроль.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов Администратор безопасности ИС обязан:

- приостановить работу ИС;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

Администратор безопасности проводит лечение зараженных файлов путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводит антивирусный контроль.

В случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, Администратор безопасности обязан запретить работу в ИС, и в возможно короткие сроки обновить пакет антивирусных программ.

9 ОРГАНИЗАЦИЯ РЕЗЕРВНОГО КОПИРОВАНИЯ

Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности информационной системы в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

Резервное копирование и хранение данных должно осуществляться на периодической основе:

– для технологической информации – не реже одного раза в месяц;

– эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Резервному копированию подлежит информация следующих основных категорий:

– персональная информация пользователей (личные каталоги) и групповая информация (общие каталоги подразделений);

– информация, обрабатываемая пользователями в ИС, а также информация, необходимая для восстановления работоспособности ИС, в т.ч. общего пользования и справочно-информационные системы общего использования;

– рабочие копии установочных компонент программного обеспечения общего назначения и специализированного программного обеспечения ИС;

– регистрационная информация системы защиты персональных данных ИС;

– другая информация, по мнению пользователей и администраторов являющаяся критичной для работоспособности ИС.

Резервное копирование информации настраивается и производится под контролем Администратора безопасности однократно после подготовки ИС к работе и хранится:

– одна копия – на локальном жестком диске;

– вторая копия – на отчуждаемом учтенном носителе.

Резервное копирование защищаемой информации (ПДн) производится еженедельно Администратором безопасности ИС.

После окончания процесса резервного копирования полученную резервную копию (архив) следует скопировать на отчуждаемый учтенный носитель.

При втором и последующих резервных копированиях текущего месяца возможно создание инкрементных архивов (если данная возможность предусмотрена в средствах резервного копирования).

В случае нехватки свободного дискового пространства для сохранения файла архива следует удалить наиболее старый архив.

На отчуждаемом носителе должны храниться архивы не менее чем за два месяца: текущий и предыдущий.

В случае необходимости восстановления данных из резервной копии, для восстановления следует использовать наиболее поздний архив. В случае невозможности использования наиболее позднего архива по каким-либо причинам, архив, используемый для восстановления, выбирается совместным решением Администратора безопасности и пользователя.

Данные о проведении процедуры резервного копирования, должны отражаться в специально созданном Журнале учета проведения процедур резервного копирования в ИС (Приложение 4).

Машинные носители информации, на которые произведено резервное копирование, должны быть учтены в Журнале учета машинных носителей для архивного копирования в ИС (Приложение 5), который находится у Администратора безопасности. В случае неотделимости носителей архивной информации от системы резервного копирования допускается их не маркировать и учитывать всю систему как одно целое.

Физический доступ к архивным копиям предоставляется только Администратору безопасности ИС.

Передача машинных носителей с архивными копиями кому бы то ни было без документального оформления не допускается.

Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

Носители должны храниться не менее одного месяца, для возможности восстановления данных.

Уничтожение отделяемых машинных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательной записью в журнале их учета.

На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, осуществляется ежедневное копирование информации, подлежащей резервированию.

В случае необходимости восстановление данных из резервных копий производится Администратором безопасности ИС.

Восстановление данных из резервных копий происходит в случае их исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

При частичном нарушении или исчезновении записей данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением настоящей Инструкции, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на Администратора безопасности ИС.

10 ПОРЯДОК ОБРАЩЕНИЯ, ХРАНЕНИЯ И УНИЧТОЖЕНИЯ МАШИННЫХ НОСИТЕЛЕЙ

При обращении с машинными носителями персональных данных (НЖМД, CD, DVD, флэш-накопители т.д.) выполняются следующие основные правила:

- находящиеся на хранении и в обращении машинные носители ПДн подлежат учёту;
- раздельному учету в журналах учета подлежат съемные носители (в том числе портативные) перезаписываемые машинные носители (флэш-накопители, съемные жесткие диски);

– пользователи для работы в ИС могут использовать только учтенные машинные носители ПДн;

– машинные носители ПДн, срок эксплуатации которых истек, уничтожаются в установленном порядке;

– все съемные носители ПДн хранятся в безопасном месте в соответствии с требованиями по их эксплуатации.

Ответственным за хранение, учет и выдачу съемных носителей ПДн является Администратор безопасности.

10.1 Порядок учета машинных носителей персональных данных

Все находящиеся на хранении и в обращении машинные носители ПДн учитываются в «Журнале учета машинных носителей персональных данных» (форма Журнала приведена в Приложении 6).

Каждый машинный носитель ПДн должен иметь этикетку, на которой указывается его регистрационный номер. В качестве регистрационных номеров допускается использовать идентификационные (серийные) номера машинных носителей, присвоенные производителем этих машинных носителей, номера инвентарного учета, в т.ч. инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

Учет и выдачу машинных носителей ПДн осуществляет Администратор безопасности. Факт выдачи и получения машинного носителя конкретным сотрудником фиксируется в соответствующем журнале учета машинных носителей персональных данных.

Учет встроенных в портативные или стационарные технические средства машинных носителей может вестись в журналах материально-технического учета в составе соответствующих технических средств. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

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

После окончания работ пользователь ИС сдает съемный носитель Администратору безопасности, о чем делается соответствующая запись в Журнале учета машинных носителей персональных данных. При наличии личного сейфа у пользователя ИС допускается хранение съемных учтенных машинных носителей в личных сейфах, в противном случае, все машинные носители ПДн должны храниться в сейфе у Администратора безопасности.

В случае передачи машинных носителей между пользователями должно обеспечиваться уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации.

В ИС должны применяться одни из следующих мер по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации:

– удаление файлов штатными средствами операционной системы и (или) форматирование машинного носителя информации штатными средствами операционной системы;

– перезапись уничтожаемых (стираемых) файлов случайной битовой последовательностью, удаление записи о файлах, обнуление журнала файловой системы или полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием.

По результатам уничтожения информации или машинного носителя комиссией составляется Акт (Приложение 7), который в последующем хранится в сейфе у Администратора безопасности ИС.

Порядок уничтожения машинных носителей персональных данных

Машинные носители ПДн, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению.

Уничтожение машинных носителей информации осуществляется комиссией по уничтожению, назначенной приказом руководителя Учреждения. Форма приказа о назначении комиссии по уничтожению машинных носителей представлена в Приложении 8.

Уничтожение магнитных, оптических, магнитооптических и электронных носителей информации производится путем их физического разрушения. Перед уничтожением носителя информация с него стирается (уничтожается), если это позволяют физические принципы работы носителя.

Перед утилизацией оборудования, участвующего в обработке ПДн, Администратором безопасности осуществляется проверка всех его компонентов, включая носители информации (жесткие диски) на отсутствие информации и лицензированного программного обеспечения (ПО).

По результатам уничтожения комиссией составляется «Акт уничтожения машинных носителей персональных данных», который в последующем хранится в сейфе у Администратора безопасности ИС, уничтоженные машинные носители информации (утилизированное оборудование) снимаются с материального учета.

11 ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ ВОЗНИКНОВЕНИЯ НЕШТАТНЫХ СИТУАЦИЙ

Общими требованиями ко всем лицам, допущенным к работе в информационной системе в случае возникновения нештатной ситуации или другого инцидента являются:

- лицо, обнаружившее нештатную ситуацию или другой инцидент, немедленно ставит в известность Администратора безопасности ИС;
- Администратор безопасности ИС обязан провести анализ ситуации и в случае невозможности исправить положение поставить в известность руководителя Учреждения. Для локализации (блокирования) проявлений угроз информационной безопасности Администратор безопасности ИС может привлекать пользователей ИС;
- по факту возникновения инцидента и выяснению причин его проявления по решению руководства может быть назначена комиссия по реагированию на инциденты информационной безопасности (далее – ИБ) и проведено служебное расследование.

12.1 Действия пользователей ИС при возникновении нештатных ситуаций

12.1.1 Сбой программного обеспечения.

Администратор безопасности выясняет причину сбоя программного обеспечения. Если привести систему в работоспособное состояние своими силами (в том числе после консультаций с разработчиками программного обеспечения) не удалось, копии акта и сопроводительных материалов (а также файлов, если это необходимо) направляются разработчику программного обеспечения для устранения причин, приведших к сбою. В случае необходимости о произошедшем инциденте Администратор безопасности сообщает руководителю Учреждения для принятия решения по существу.

12.1.2 Отключение электропитания технических средств ИС.

Администратор безопасности ИС проводит анализ на наличие потерь и (или) разрушения данных и программного обеспечения, а также проверяет работоспособность оборудования. В случае необходимости производится восстановление программного обеспечения и данных из последней резервной копии с составлением акта. При

необходимости о произошедшем инциденте Администратор безопасности ИС сообщает руководителю Учреждения для принятия решения по существу.

12.1.3 Выход из строя технических средств ИС (рабочих станций, серверов, источников бесперебойного питания, программно-аппаратных средств межсетевого экранирования и т.д.).

Администратор безопасности выполняет мероприятия по ремонту неисправного технического средства информационной системы.

При необходимости производятся работы по восстановлению программного обеспечения из эталонных копий с составлением акта.

12.1.4 Обнаружение вредоносной программы в программной среде средств автоматизации ИС.

При обнаружении вредоносной программы (ВП) производится ее локализация с целью предотвращения ее дальнейшего распространения. При этом зараженную рабочую станцию рекомендуется физически отсоединить от локальной вычислительной сети ИС, и Администратор безопасности проводит анализ состояния рабочей станции.

После ликвидации ВП проводится внеочередная проверка на всех элементах ИС с применением обновленных антивирусных баз. При необходимости производится восстановление программного обеспечения из эталонных копий с составлением акта.

По факту появления ВП в локальной вычислительной сети может быть проведено служебное расследование. Решение о необходимости проведения служебного расследования принимается руководителем Учреждения.

12.1.5 Утечка информации.

При обнаружении утечки информации ставится в известность Администратор безопасности ИС. По факту может быть проведена процедура служебного расследования. Если утечка информации произошла по техническим причинам, проводится анализ защищенности процессов ИС и, если необходимо, принимаются меры по устранению каналов утечки и предотвращению их возникновения.

12.1.6 Взлом операционной системы средств автоматизации ИС (несанкционированное получение доступа к ресурсам операционной системы).

При обнаружении взлома рабочей станции ставится в известность Администратор безопасности ИС.

По возможности производится временное отключение рабочей станции от локальной вычислительной сети ИС для проверки на наличие ВП.

Администратором безопасности проверяется целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения, проводится анализ состояния файлов - скриптов и журналов сервера, производится смена всех паролей, которые имели отношение к данной рабочей станции.

В случае необходимости производится восстановление программного обеспечения из эталонных копий с составлением акта.

По результатам анализа ситуации проверяется вероятность проникновения несанкционированных программ в ИС, после чего проводятся аналогичные работы по проверке и восстановлению программного обеспечения и данных на других информационных узлах ИС.

12.1.7 Попытка несанкционированного доступа (НСД).

При попытке НСД Администратором безопасности ИС проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД. По результатам анализа, в случае необходимости (есть реальная угроза НСД), принимаются меры по предотвращению НСД.

Проводится внеплановая смена паролей. В случае появления обновлений программного обеспечения, устраняющих уязвимости системы безопасности, Администратором безопасности ИС устанавливаются такие обновления.

По факту обнаружения попытки НСД может быть проведено служебное

расследование. Решение о необходимости проведения служебного расследования принимается руководителем Учреждения.

В случае установления в ходе служебного расследования факта осуществления попытки НСД со стороны внешних по отношению к ИС субъектов, лицами, уполномоченными на проведение такого расследования, принимаются меры по фиксации и документированию факта инцидента и готовятся материалы для передачи в компетентные органы дознания для проведения предварительного расследования, установления субъекта-нарушителя, определения наличия состава преступления и принятия решения о возбуждении уголовного дела.

12.1.8 Компрометация ключевой информации (паролей доступа).

При компрометации ключевой информации (пароля доступа) Администратором безопасности проводится внеплановая смена пароля в соответствии с требованиями к организации парольной защиты, установленными настоящими Правилами, анализируется ситуация на наличие последствий компрометации и принимаются необходимые меры по минимизации возможного (или нанесенного) ущерба.

12.1.9 Физическое повреждение или хищение оборудования технических средств ИС.

Сотрудником, обнаружившим физическое повреждение элементов ИС, ставится в известность Администратор безопасности ИС.

Администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяется причина повреждения элементов ИС и возможные угрозы информационной безопасности.

О факте повреждения элементов ИС в случае необходимости Администратор безопасности докладывает руководителю Учреждения.

В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование.

Администратором безопасности ИС проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

При необходимости Администратором безопасности ИС проводятся мероприятия по восстановлению программного обеспечения из эталонных копий с составлением акта.

12.1.10 Невыполнение установленных правил ИБ (правил работы в ИС), использование ИС с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации.

Сотрудником, обнаружившим невыполнение установленных правил ИБ, использование ИС с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации, ставится в известность Администратор безопасности ИС.

Администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента.

Об обнаруженном факте Администратор безопасности ИС в случае необходимости докладывает руководителю Учреждения.

По решению руководителя Учреждения по фактам выявленных нарушений может быть проведено служебное расследование.

12.1.11 Ошибки сотрудников.

В случае возникновения сбоя, связанного с ошибками сотрудников, Администратором безопасности ИС проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента и необходимость восстановления программного обеспечения.

При необходимости Администратором безопасности ИС проводятся мероприятия по

восстановлению программного обеспечения и данных из эталонных копий с составлением акта.

В случае нанесения значительного ущерба вследствие ошибок работников по решению руководителя Учреждения может быть проведено служебное расследование.

12.1.12 Отказ в обслуживании.

Сотрудником, обнаружившим отказ в обслуживании, ставится в известность Администратор безопасности ИС.

Администратором безопасности проводится анализ с целью определения причин, вызвавших отказ в обслуживании.

Администратором безопасности проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

При необходимости, проводятся мероприятия по восстановлению программного обеспечения с составлением акта.

О причинах инцидента и принятых мерах Администратор безопасности ИС информирует руководителя Учреждения.

12.1.13 Несанкционированные изменения состава программных и аппаратных средств (конфигурации) ИС.

В случае обнаружения несанкционированного изменения состава программных и аппаратных средств (конфигурации) ИС Администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы ИБ в результате инцидента.

Администратором безопасности проводятся мероприятия по восстановлению программного обеспечения, а также (при необходимости) проверка на наличие компьютерных ВП.

12.1.14 Техногенные и природные проявления нештатных ситуаций.

При стихийном бедствии, пожаре или наводнении, грозящем уничтожению или повреждению информации (данных), сотруднику, обнаружившему факт возникновения нештатной ситуации необходимо:

– немедленно оповестить других сотрудников и принять все меры для самостоятельной оперативной защиты помещения;

– немедленно позвонить в соответствующие службы помощи (пожарная охрана, служба спасения и т.д.);

– немедленно сообщить Администратору безопасности ИС.

После оперативной ликвидации причин, вызвавших пожар или наводнение, может быть назначена внутренняя комиссия по устранению последствий инцидента.

Комиссия определяет ущерб (состав и объем уничтоженных оборудования и информации) и причины, по которым произошло происшествие, а также выявляет виновных.

12 ПОРЯДОК ИЗМЕНЕНИЯ СОСТАВА И КОНФИГУРАЦИИ ТЕХНИЧЕСКИХ И ПРОГРАММНЫХ СРЕДСТВ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Все изменения в конфигурации технических и программных средств ИС должны производиться только после их согласования с организацией, выдавшей Аттестат соответствия на ИС.

Для внесения изменений в состав и конфигурацию технических и программных средств ИС составляется заявка (Приложение 9) на имя руководителя организации, выдавшей Аттестат соответствия на ИС, которая им рассматривается.

В заявке могут указываться следующие виды необходимых изменений в составе технических и программных средств ИС:

- добавление устройства (узла, блока) в состав ИС;
- замена устройства (узла, блока) в составе ИС;
- изъятие устройства (узла, блока) из состава ИС;
- обновление (замена) программных средств;
- удаление из ИС программных средств.

Право внесения изменений в конфигурацию технических и программных средств ИС предоставляется Администратору безопасности на основании распоряжения руководителя Учреждения.

Все добавляемые технические и программные средства должны быть предварительно установленным порядком проверены на работоспособность, а также на отсутствие опасных функций.

После установки (обновления) ПО, Администратор безопасности должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с ее (его) эксплуатационной документацией и проверить работоспособность ПО и правильность настройки средств защиты.

После завершения работ по внесению изменений в состав аппаратных средств, системный блок должен закрываться администратором безопасности и опечатываться (пломбироваться или защищаться специальной наклейкой).

Внесение изменений в составе технических и программных средств происходит с обязательным документированием, разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

В случае, если планируемые изменения могут быть внесены на объекте информатизации без дополнительной проверки эффективности системы защиты персональных данных, необходимо:

1. Составить распоряжение/приказ руководителя Учреждения о внесении изменений в составе ИС.

2. Составить соответствующий акт изменений в составе ИС в произвольной форме.

3. Внести отметку в пункте «Лист регистрации изменений» технического паспорта ИС с указанием порядкового № и даты введения изменений, наименования документа, фиксирующего изменения; № замененных (исправленных) листов технического паспорта, зафиксировать внесенные изменения подписью внесшего их лица. При внесении изменений в технический паспорт прежняя соответствующая запись (раздел, строка или позиция паспорта) гасится, а рядом со штампом «Погашено» ставится штамп (или рукописная запись) «См. изменение N _____». Номер при этом должен соответствовать номеру записи в Листе регистрации изменений Технического паспорта. Все изменения вписываются в «Лист регистрации изменений» Технического паспорта в хронологическом порядке их выявления под соответствующим номером. Ссылка на номер записи, имеющаяся в техническом паспорте при этом сохраняется.

В случае, если планируемые изменения требуют дополнительной проверки эффективности системы защиты персональных данных, необходимо действовать в соответствии с указаниями, полученными от организации, выдавшей Аттестат соответствия.

13 ЗАЩИТА ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

События безопасности, подлежащие регистрации в ИС, определяются с учетом способов реализации угроз безопасности информации. К событиям безопасности, подлежащим регистрации в ИС, относятся любые проявления состояния информационной системы и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности

компонентов ИС, нарушения процедур, установленных организационно-распорядительными документами по защите информации, а также нарушения штатного функционирования средств защиты информации.

В ИС определены следующие события безопасности, подлежащие регистрации:

1. События, связанные с регистрацией входа (выхода) субъектов доступа в систему или загрузки операционной системы. Состав и содержание информации включают дату и время входа (выхода) в систему (из системы) или загрузки операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

2. События, связанные с регистрацией подключения машинных носителей информации и вывода информации на носители информации. Состав и содержание регистрационных записей включает: дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, подключившего машинный носитель или осуществляющего вывод информации на носитель информации.

3. События, связанные с регистрацией запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации. Состав и содержание регистрационных записей включает: дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

4. События, связанные с регистрацией попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. Состав и содержание регистрационных записей включает: дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

5. События, связанные с регистрацией попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам). Состав и содержание информации должны включать: дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

6. События, связанные с регистрацией запланированного обновления антивирусных баз. Состав и содержание информации должны включать дату и время обновления.

7. События, связанные с регистрацией запланированного обновления ОС Windows. Ведутся в журнале самой ОС. Состав и содержание информации должны, включать дату и время обновления, состав обновления.

События безопасности, подлежащие регистрации в ИС, и сроки хранения соответствующих записей регистрационных журналов, обеспечивают возможность обнаружения, идентификации и анализа инцидентов, возникших в ИС.

Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется Администратором безопасности, исходя из возможностей реализации угроз безопасности информации.

Срок хранения информации о зарегистрированных событиях безопасности должен составлять не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации.

Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в соответствии с методическими

документами, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

Доступ к записям аудита и функциям управления механизмами регистрации (аудита) средств защиты информации (далее – СЗИ) предоставляется только Администратору безопасности ИС.

В ИС для обеспечения защиты информации о событиях безопасности, перед установкой СЗИ осуществляется синхронизация системного времени и даты. Администратор безопасности осуществляет контроль неизменности установленного системного времени и проводит периодическую проверку журналов регистрации событий, для контроля правильности отображения временных меток.

Сбор, запись и хранение информации о событиях безопасности осуществляется с помощью встроенных средств операционной системы Windows и установленных СЗИ.

В целях предотвращения сбоев при регистрации событий безопасности СЗИ и операционной системы в ИС:

1. Администратору безопасности ИС необходимо еженедельно проверять журналы регистрации событий СЗИ и операционной системы на наполненность и, в случае необходимости, производить их архивацию.
2. Увеличить при необходимости объем выделяемой под журналы событий безопасности СЗИ и операционной системы памяти.
3. Включить автоматическую перезапись новых событий безопасности поверх устаревших для предотвращения возникновения ошибок переполнения журналов.
4. Настройки прав учетных записей пользователей ИС должны исключать возможность внесения пользователями изменений в журналы событий безопасности, настройки СЗИ и операционной системы.
5. При появлении в ИС ошибок операционной системы или СЗИ пользователю необходимо уведомить Администратора безопасности и по возможности приостановить работу до устранения ошибки.

14 МЕРОПРИЯТИЯ ПО КОНТРОЛЮ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И РАБОТОЙ ПОЛЬЗОВАТЕЛЕЙ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Контрольные мероприятия за обеспечением уровня защищенности и соблюдения условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке защищаемой информации, в т.ч. ПДн, в ИС проводятся в следующих целях:

- проверка выполнения требований организационно-распорядительной документации по защите информации в ИС и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;
- оценка уровня осведомленности и знаний работников, допущенных к работе в ИС, в области обработки и защиты персональных данных;
- оценка обоснованности и эффективности применяемых мер и средств защиты.

14.1 Тематика внутреннего контроля

Проверки соответствия обработки ПДн в ИС установленным требованиям разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

Регулярные контрольные мероприятия проводятся Администратором безопасности ИС периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, Приложение 10) и предназначены для осуществления

контроля выполнения требований в области защиты ПДн.

Плановые контрольные мероприятия проводятся комиссией периодически в соответствии с утвержденным Планом и направлены на постоянное совершенствование системы защиты персональных данных ИС.

Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (создается на период проведения мероприятий). Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

- по результатам расследования инцидента информационной безопасности;
- по результатам внешних контрольных мероприятий, проводимых регулирующими органами;
- по решению руководителя Учреждения.

14.2 Планирование контрольных мероприятий

Для проведения плановых внутренних контрольных мероприятий Администратор безопасности разрабатывает План внутренних контрольных мероприятий на текущий год.

План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий: состав участников, привлекаемых для проведения контрольных мероприятий, сроки и этапы проведения контрольных мероприятий.

Общий срок контрольных мероприятий не должен превышать пять рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Протоколе, выполняемом по результатам проведенных контрольных мероприятий.

14.3 Оформление результатов контрольных мероприятий

По итогам проведения плановых и внеплановых контрольных мероприятий ответственное лицо или комиссия разрабатывает Протокол (Приложение 11), в котором указывается:

- описание проведенных мероприятий по каждому из этапов;
- перечень и описание выявленных нарушений;
- рекомендации по устранению выявленных нарушений;
- заключение по итогам проведения внутреннего контрольного мероприятия.

Протокол передается на рассмотрение руководителю Учреждения.

Общая информации о проведенном контрольном мероприятии фиксируется в «Журнале учета внутренних мероприятий по контролю за обеспечением безопасности ПДн при их обработке в ИС» (Приложение 12).

14.4 Порядок проведения плановых и внеплановых контрольных мероприятий

Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственного за организацию обработки ПДн в Учреждении совместно с Администратором безопасности ИС (далее - комиссия).

Проверки соответствия обработки ПДн установленным требованиям в ИС проводятся на основании Плана проведения контрольных мероприятий.

Проведение внеплановой проверки организуется в течение пяти рабочих дней с момента поступления соответствующего заявления.

При проведении проверки соответствия обработки ПДн установленным требованиям должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИС, исполнение которых обеспечивает установленный уровень защищенности ПДн;
- порядок и условия применения средств защиты информации;

– эффективность принимаемых мер по обеспечению безопасности ПДн при их обработке в ИС;

– состояние учета машинных носителей ПДн;

– соблюдение правил доступа к персональным данным;

– наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер.

14.5 При проведении внутренней проверки комиссия имеет право:

– запрашивать у сотрудников Учреждения, допущенных к обработке ПДн в ИС, сведения, необходимые для реализации полномочий;

– требовать от уполномоченных на обработку ПДн должностных лиц уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем ПДн;

– принимать меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований законодательства Российской Федерации;

– вносить руководителю Учреждения предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности ПДн предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки ПДн.

В отношении информации ограниченного доступа, ставшей известной комиссии в ходе проведения мероприятий по внутреннему контролю, должна обеспечиваться ее конфиденциальность.

Проверка должна быть завершена не позднее, чем через пять рабочих дней со дня принятия решения о её проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений составляется Протокол, который должен быть представлен руководителю Учреждения для ознакомления.

Все проводимые мероприятия по контролю за обеспечением безопасности персональных данных должны быть зафиксированы в «Журнале учета внутренних мероприятий по контролю за обеспечением безопасности ПДн при их обработке в ИС». Ответственность за ведение Журнала возлагается на Администратора безопасности ИС.

15 ОБЕСПЕЧЕНИЕ ФУНКЦИОНИРОВАНИЯ И БЕЗОПАСНОСТИ КРИПТОСРЕДСТВ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Ответственный за обеспечение функционирования и безопасности криптосредств назначается приказом руководителя Учреждения из числа пользователей криптосредств, или его обязанности возлагаются на структурное подразделение или должностное лицо (работника), ответственных за защиту информации (обеспечение безопасности персональных данных).

СКЗИ должны использоваться для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

15.1 Порядок получения допуска пользователей к работе с СКЗИ

Для работы пользователей с СКЗИ в ИС необходимо реализовать ряд мероприятий:

Пользователи, которым необходимо получить доступ к работе с СКЗИ, должны быть проинструктированы и обучены правилам работы с СКЗИ;

Учёт лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения защиты информации в ИС, осуществлять в Перечне пользователей СКЗИ;

Контроль над реализацией данных мероприятий возлагается на Ответственного за обеспечение функционирования и безопасности криптосредств.

15.2 Обязанности Ответственного

При решении всех вопросов, связанных с обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа, Ответственный должен руководствоваться Инструкцией по обращению с СКЗИ в ИС.

На Ответственного возлагается проведение следующих мероприятий:

– ведение Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (Приложение 13);

– принятие СКЗИ, эксплуатационной и технической документации к ним, ключевых документов от пользователя при его увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

– осуществление периодической проверки журнала учета СКЗИ, перечня пользователей СКЗИ и иных документов.

Ответственный обязан:

– не разглашать информацию ограниченного доступа, к которой он допущен, в том числе сведения о криптоключах;

– сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;

– соблюдать требования к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;

– контролировать целостность печатей (пломб) на технических средствах с установленными СКЗИ;

– немедленно уведомлять руководителя Учреждения о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах компрометации криптоключей, которые могут привести к разглашению информации ограниченного доступа, а также о причинах и условиях возможной утечки такой информации;

– незамедлительно принимать меры по локализации последствий компрометации защищаемых сведений конфиденциального характера;

– не допускать ввод одного номера лицензии на право использования СКЗИ более чем на одно рабочее место.

15.3 Права Ответственного

В рамках исполнения возложенных на него обязанностей, Ответственный имеет право:

– требовать от пользователей СКЗИ соблюдения положений настоящих правил по обращению с СКЗИ;

– обращаться к руководителю Учреждения с требованием прекращения работы пользователя с СКЗИ при невыполнении им установленных требований по обращению с СКЗИ;

– инициировать проведение служебных расследований по фактам нарушения в Учреждении порядка обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

15.4 Порядок передачи обязанностей при смене Ответственного

При смене Ответственного должны быть внесены соответствующие изменения в Приказ об обращении с СКЗИ. Вновь назначенный Ответственный должен быть ознакомлен под роспись с настоящей Инструкцией и приступить к исполнению возложенных на него обязанностей.

15.5 Общий порядок работы с СКЗИ

Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ. На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае, в Учреждении должны быть обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется, после получения ключевых носителей, создать рабочие копии. Копии должны быть соответствующим образом маркированы и должны использоваться, учитываться и храниться так же, как оригиналы.

Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ под расписку в соответствующих журналах поэкземплярного учета.

При обнаружении на рабочем месте, оборудованном СКЗИ, посторонних программ или вирусов, нарушающих работу указанных средств, работа со средствами защиты информации на данном рабочем месте должна быть прекращена и организуются мероприятия по анализу и ликвидации негативных последствий данного нарушения.

15.6 Действия в случае компрометации ключей

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации ограниченного доступа, пользователи СКЗИ обязаны сообщать Ответственному за обеспечение функционирования и безопасности криптосредств.

К компрометации ключей относятся следующие события:

утрата носителей ключа;

утрата иных носителей ключа с последующим обнаружением;

увольнение сотрудников, имевших доступ к ключевой информации;

возникновение подозрений на утечку информации или ее искажение;

нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;

утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;

утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;

доступ посторонних лиц к ключевой информации;

другие события утери доверия к ключевой документации.

Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия.

Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения). В случаях недостачи, не предъявления ключевых документов, а также неопределенности их местонахождения

принимаются срочные меры к их розыску.

Мероприятия по розыску и локализации последствий компрометации информации ограниченного доступа, передававшейся (хранящейся) с использованием СКЗИ, организует и осуществляет Учреждение (обладатель скомпрометированной информации ограниченного доступа).

15.7 Обязанности пользователей СКЗИ

Пользователи СКЗИ обязаны:

– не разглашать информацию ограниченного доступа, к которой они допущены, в том числе сведения о криптоключах;

– сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;

– соблюдать требования к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;

– сообщать Ответственному за функционирование и обеспечение безопасности криптосредств о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

– сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

– немедленно уведомлять Ответственного за функционирование и обеспечение безопасности криптосредств о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

Пользователь несет ответственность за то, чтобы на ПК, на котором установлены СКЗИ, не были установлены и не эксплуатировались программы (в том числе, программы-вирусы), которые могут нарушить функционирование СКЗИ.

На ПК, оборудованном СКЗИ, программное обеспечение должно быть лицензионным. При обнаружении на ПК, оборудованном СКЗИ, посторонних программ или вирусов, работа с СКЗИ на данном рабочем месте должна быть прекращена и организованы мероприятия по анализу и ликвидации негативных последствий данного нарушения.

Все полученные обладателем информации ограниченного доступа экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность.

Не допускается:

– разглашать информацию ограниченного доступа, к которой был допущен пользователь СКЗИ;

– разглашать содержимое ключевых носителей или передавать сами носители лицам, к ним не допущенным;

– выводить ключевую информацию на дисплей и(или) принтер;

– вставлять ключевой носитель в порт ПК при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной цифровой подписи и т.д.), а также в порты других ПК;

– записывать на ключевом носителе постороннюю информацию;

– вносить какие-либо изменения в программное обеспечение СКЗИ;

– использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей).

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации ограниченного доступа, пользователи СКЗИ обязаны сообщать Ответственному за функционирование и обеспечение безопасности криптосредств.

15.8 Ответственность пользователей СКЗИ

Пользователи СКЗИ отвечают за исполнение своих функциональных обязанностей и сохранность информации ограниченного доступа, которая стала ему известной вследствие исполнения им своих служебных обязанностей. Ответственность лиц, допущенных к работе с СКЗИ, за неисполнение и/или ненадлежащее исполнение своих обязанностей, предусмотренных соответствующими разделами настоящих Правил, а также за разглашение информации ограниченного доступа, ставшей ему известной вследствие исполнения им своих служебных обязанностей, определяется действующим законодательством Российской Федерации и условиями трудового договора.

16 РАБОТА СО СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ

В качестве средств защиты информации от несанкционированного доступа на АРМ используются сертифицированные ФСТЭК России СЗИ от НСД «Dallas Lock 8.0-K».

Сертификат соответствия ФСТЭК России № 2720 от 25.09.2012 г. удостоверяет, что система защиты информации от несанкционированного доступа «Dallas Lock 8.0-K», разработанная и производимая ООО «Конфидент» в соответствии с техническими условиями RU.48957919.501410-01 91, функционирующая в средах операционных систем, указанных в формуляре RU.48957919.501410-01 30, является программным средством защиты информации от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, соответствует требованиям руководящих документов «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по 5 классу защищенности, «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа» (Гостехкомиссия России, 1997) – по 3 классу защищенности, «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по 4 уровню контроля, документа «Требования к средствам контроля съемных машинных носителей информации» (ФСТЭК России, 2014) – по 4 классу защиты, методического документа «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.П4.ПЗ» при выполнении ограничений, указанных в формуляре.

16.1. Вход в операционную систему

При загрузке компьютера, защищенного СЗИ НСД Dallas Lock 8.0-K, в зависимости от операционной системы, появляется экран приветствия (приглашение на вход в операционную систему) (Рисунок 1).

Рисунок 1. Экран приветствия в ОС Windows 7

Для входа на защищенный СЗИ НСД Dallas Lock 8.0-К компьютер каждому пользователю предлагается выполнить следующую последовательность шагов:

1. Заполнить поле имени пользователя, под которым он зарегистрирован в системе защиты. В зависимости от настроек в этом поле может оставаться имя пользователя, выполнившего вход последним.

2. Заполнить поле имени домена. Если пользователь доменный, то указывается имя домена, если пользователь локальный, то в этом поле оставляется имя компьютера или оставляется пустое значение.

3. Если пользователю назначен аппаратный идентификатор, то его необходимо предъявить (подробное описание приводится ниже).

4. Ввести пароль. При вводе пароля, поле для ввода является текстовым. Однако на экране вместо символа, соответствующего каждой нажатой клавише, появляется символ «●» (точка).

При вводе пароля следует помнить, что строчные и прописные буквы различаются. Допущенные ошибки при вводе исправляются так же, как и при заполнении текстового поля.

5. Нажать кнопку «Enter».

После нажатия кнопки «Enter» осуществляется проверка наличия в системе защиты зарегистрированного пользователя с указанным именем. После чего проверяется соответствие с именем пользователя, зарегистрированного в системе защиты, и правильность указанного пользователем пароля. В случае успеха проверки пользователю разрешается вход.

Попытка входа пользователя на защищенный компьютер может быть неудачной, к чему приводит ряд событий. При этом на экран могут выводиться сообщения о характере события или соответствующие сообщения предупреждающего характера. Если введенный пароль неверен, то на экране появится сообщение об ошибке, после чего система защиты предоставит возможность повторно ввести имя и пароль (Рисунок 2).

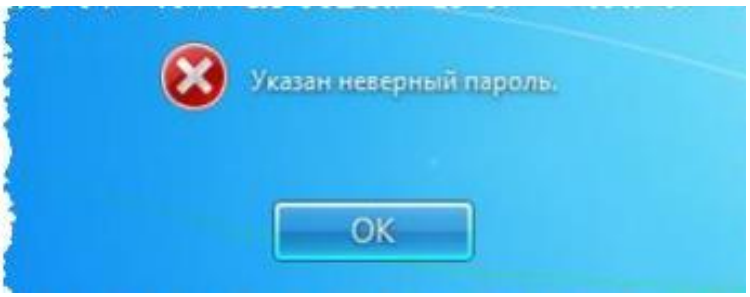


Рисунок 2. Сообщение при вводе неправильного пароля

Возможна ситуация, при которой пользователь забыл свой пароль. В этом случае он также должен обратиться к администратору безопасности, который имеет право назначить пользователю новый пароль. Так же при ошибочном вводе данных в поле имени или домена могут возникнуть соответствующие сообщения (Рисунок 3).

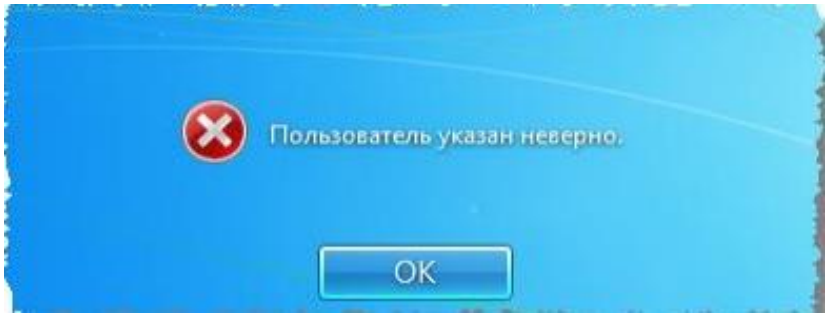


Рисунок 3. Ошибка авторизации

На этапе загрузки компьютера осуществляется контроль целостности аппаратно-программной среды BIOS, поэтому может быть выведено предупреждение о нарушении данных параметров. После ввода имени и пароля на этапе загрузки компьютера на экране может появиться предупреждение о том, что нарушен контроль целостности, вход в операционную систему для пользователя будет запрещен (Рисунок 4).

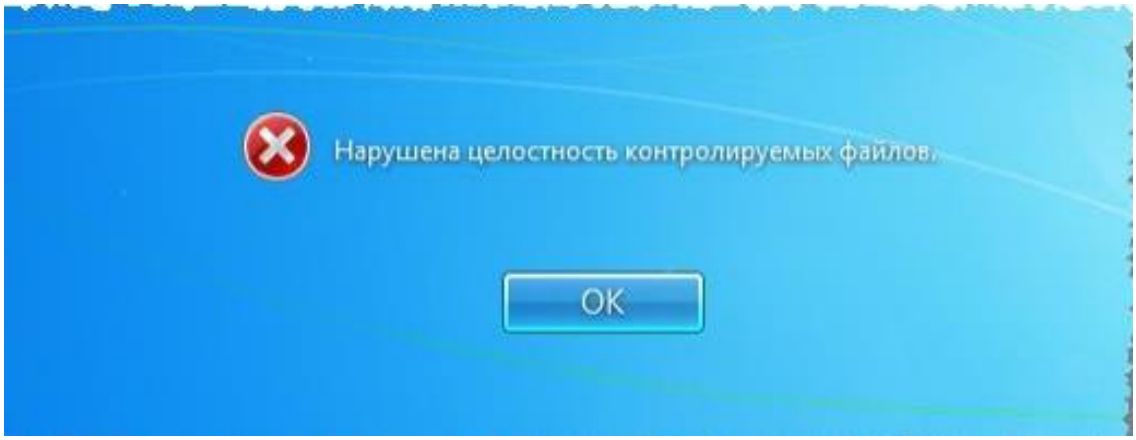


Рисунок 4. Сообщение о нарушении целостности контролируемых файлов

В случае возникновения данной ошибки пользователю необходимо обратиться к Администратору безопасности.

16.2 Завершение работы

При завершении сеанса работы пользователя на компьютере, например, в конце рабочего дня, необходимо выполнить стандартное выключение компьютера. Для этого нужно:

1. Сохранить все данные и завершить работу всех приложений, так как выключение не сохраняет результатов работы.

2. В меню «Пуск»  нижнем правом углу нажать кнопку «Завершение работы».

3. После нажатия кнопки «Завершение работы» компьютер закрывает все открытые программы, вместе с самой ОС Windows, а затем полностью выключает компьютер и монитор.

16.3 Смена пользователя

Возможно, что завершение сеанса пользователя необходимо для смены пользователя компьютера, то есть для входа на данный компьютер под другой учетной записью. Для завершения сеанса и смены пользователя, в зависимости от версии операционной системы, необходимо сделать следующее:

1. В ОС Windows 7  в меню «Пуск» в нижнем правом углу нажать вызов меню возле кнопки «Завершение работы» и выбрать пункт «Сменить пользователя» (Рисунок 5).

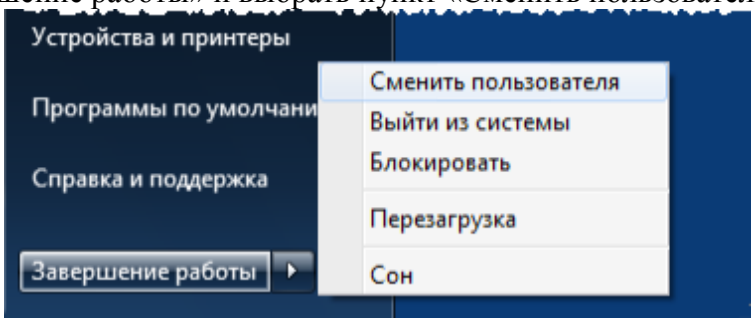
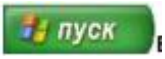


Рисунок 5. Смена пользователя в ОС Windows 7

2. В ОС Windows XP в меню «Пуск»  в нижнем правом углу нажать кнопку «Завершение работы» и в появившемся окне выбрать пункт меню «Завершение сеанса …» (Рисунок 6).

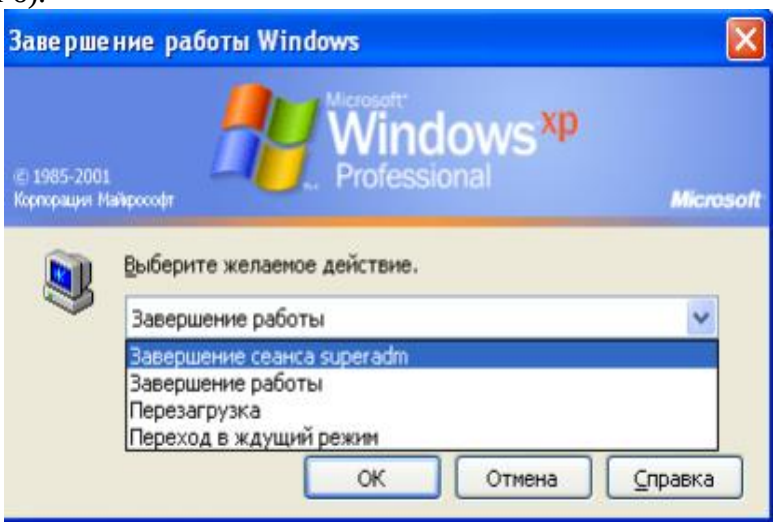


Рисунок 6. Смена пользователя в ОС Windows XP

Сеанс текущего пользователя будет завершен, а на экране появится диалог для повторной авторизации в системе защиты.

При смене сеанса пользователя, хотя выход пользователя и происходит, но на компьютере продолжают работать все запущенные им приложения. Перед сменой пользователя рекомендуется сохранить все необходимые данные и закончить работу приложений.

16. 4 Смена пароля

Смена пароля должна осуществляться не реже одного раза в 90 дней.

Пользователь может самостоятельно сменить свой пароль для авторизации.

1. Для этого, после входа в операционную систему, необходимо нажать комбинацию клавиш «Ctrl-Alt-Del» и выбрать операцию «Сменить пароль» (Рисунок 7).

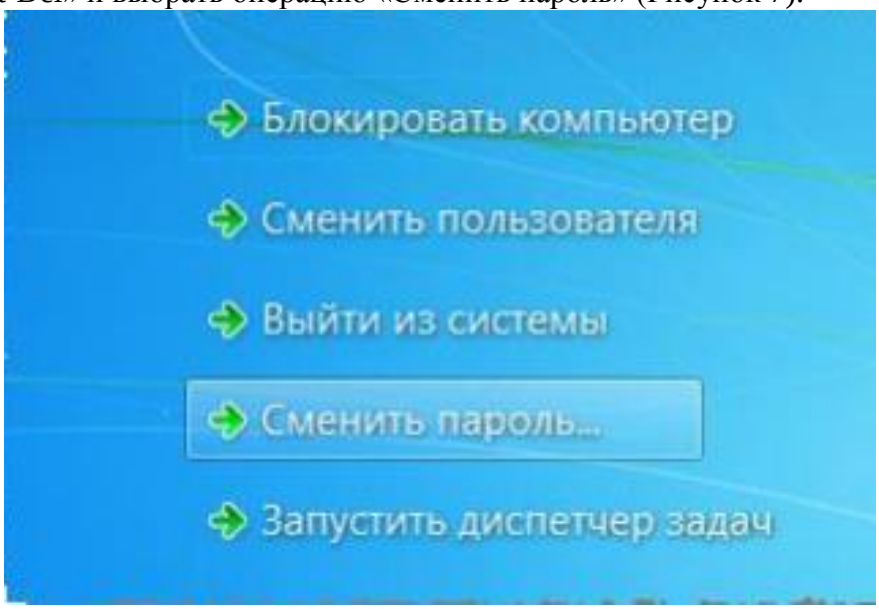


Рисунок 7. Меню действий

На экране появится диалоговое окно, предлагающее ввести данные для смены пароля (Рисунок 8).

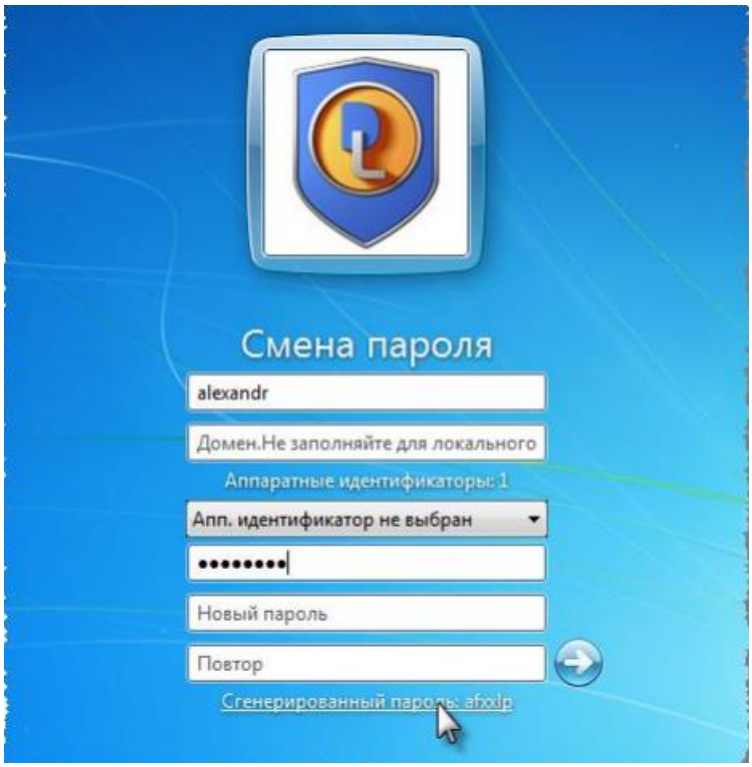


Рисунок 8. Экран смены пароля

2. В открывшемся диалоговом окне необходимо ввести в соответствующие поля имя

пользователя, имя домена (для доменного пользователя, для локального – оставить это поле пустым), старый пароль, новый пароль и подтверждение нового пароля.

3. Далее нажать кнопку «ОК» для сохранения нового пароля или кнопку «Отмена».

Если все требования соблюдены, то пароль пользователя будет успешно сменен, появится соответствующее сообщение (Рисунок 9)

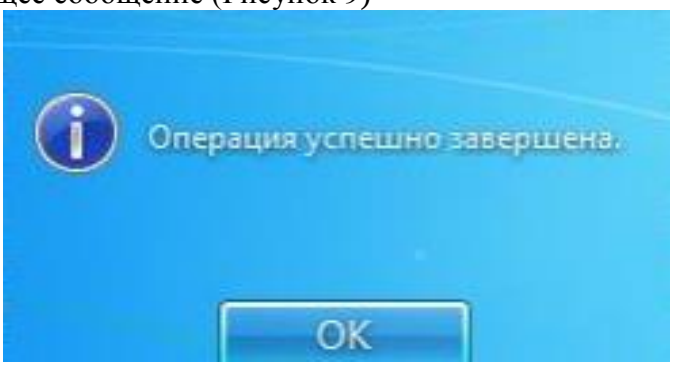


Рисунок 9. Подтверждение о смене пароля

Далее вход пользователя на защищенную СЗИ НСД Dallas Lock 8.0-К рабочую станцию будет осуществляться с новым паролем.

17 РАБОТА С МОБИЛЬНЫМИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

В качестве мобильных технических средств в ИС определены ноутбуки.

Мобильные технические средства предназначены для предоставления сотрудникам Учреждения локального доступа к информационным ресурсам ИС.

К использованию на мобильных технических средствах допускается только программное обеспечение, обозначенное в Перечне программного обеспечения и (или) его компонентов, разрешенного к использованию на ПЭВМ, входящих в состав ИС, утвержденного руководителем Учреждения. Установка, мониторинг и сопровождение программного обеспечения мобильных технических средств осуществляется администратором безопасности в рамках возложенных на него обязанностей.

Для использования в ИС допускаются только учтенные мобильные технические средства, являющиеся собственностью Учреждения. Инвентаризация мобильных технических средств проводится в соответствии с процедурами и механизмами контроля, принятыми в Учреждении.

Подключение пользователей мобильных технических средств и назначение им необходимых полномочий осуществляется в соответствии с настоящими Правилами.

Подключение мобильных технических средств к ресурсам ИС осуществляется с использованием сертифицированных средств защиты информации, принятых в эксплуатацию в ИС.

Средства защиты информации должны быть предустановлены до начала эксплуатации мобильных технических средств.

Параметры настройки общесистемного программного обеспечения и программного обеспечения средств защиты информации, должны обеспечивать реализацию мер защиты информации, а также устранение возможных уязвимостей, приводящих к возможности появления угроз безопасности информации.

В случае отсутствия установленных средств защиты информации, несоответствия настроек средств защиты информации и операционной системы мобильного технического средства необходимым параметрам безопасности, доступ к ресурсам ИС должен быть запрещен.

В случае передачи мобильного технического средства другому пользователю

администратором безопасности, в рамках возложенных на него обязанностей, проводится очистка пользовательской информации (загруженных данных, истории просмотра и т.д.) и заведение новой учетной записи.

В случае вывода мобильного технического средства из эксплуатации (при невозможности ремонта и очистки информации) выполняется физическое уничтожение мобильного технического средства в установленном порядке и смена учетных данных пользователя мобильного технического средства.

Мобильные технические средства должны использоваться сотрудниками Учреждения только для выполнения служебных обязанностей.

Не допускается:

– использование мобильных технических средств в личных целях;

– самостоятельное внесение изменений в состав программного обеспечения мобильных технических средств;

– перенос информации ограниченного доступа на неучтенные машинные носители информации;

– использование карт памяти, подключаемых к мобильным техническим средствам для хранения и передачи информации ограниченного доступа;

– вынос мобильных технических средств за пределы помещений, в которых расположены элементы ИС.

18 РАБОТА С БЕСПРОВОДНЫМ ДОСТУПОМ

В качестве средств беспроводного доступа в ИС СО могут использоваться USB-модемы, беспроводные устройства вода информации (клавиатура, мышь), Wi-Fi сети.

Мониторинг, управление и сопровождение систем беспроводного доступа осуществляется Администратором безопасности.

Доступ к беспроводной сети осуществляется на основе использования учетных записей пользователей, указанных в разрешительной системе доступа.

Обязанностью пользователя является сохранение своих сетевых реквизитов (логина и пароля) в тайне от посторонних лиц. Использование одной учётной записи для одновременных сеансов работы в беспроводной сети ограничивается. Использование чужих учётных записей для доступа к беспроводной сети запрещено.

Пользователь несет персональную ответственность за целесообразность использованного объема входящего и исходящего трафика и за содержание информации, полученной или переданной с использованием технологий беспроводного доступа.

Использование сетей беспроводного доступа возможно только с включенными средствами защиты используемыми в ИС.

Средства беспроводного доступа должны использоваться сотрудниками Учреждения только для выполнения служебных обязанностей.

19 ПОРЯДОК ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ВЫВОДЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ИЗ ЭКСПЛУАТАЦИИ ИЛИ ПОСЛЕ ПРИНЯТИЯ РЕШЕНИЯ ОБ ОКОНЧАНИИ ОБРАБОТКИ ИНФОРМАЦИИ

Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации осуществляется Оператором ИС, в соответствии с организационно-распорядительными документами по защите информации, и в том числе включает:

архивирование информации, содержащейся в информационной системе;

гарантированное уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

Архивирование информации, содержащейся в информационной системе, должно

осуществляться при необходимости дальнейшего использования информации в деятельности пользователя.

Гарантированное уничтожение (стирание) данных и остаточной информации с машинных носителей информации, производится при необходимости передачи машинного носителя другому пользователю информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации в соответствии с утвержденным порядком.

Ответственность за соблюдение требований по обеспечения защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации возлагается на Администратора безопасности.

ПРИЛОЖЕНИЯ