ПРАВИТЕЛЬСТВО СВЕРДЛОВСКОЙ ОБЛАСТИ
МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ СВЕРДЛОВСКОЙ ОБЛАСТИ

ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ СВЕРДЛОВСКОЙ ОБЛАСТИ «УРАЛЬСКИЙ КОЛЛЕДЖ СТРОИТЕЛЬСТВА, АРХИТЕКТУРЫ И ПРЕДПРИНИМАТЕЛЬСТВА» (ГАОУ СПО СО «УКСАП»)

Документ подписан электронной подписью

Владелец: ГАПОУ СО "Уральский колледж строительства, архитектуры и предпринимательства" ГАПОУ СО "УКСАП"
Бурганова Ольга Владимировна
620078, Свердловская обл, г. Екатеринбург, ул. Малышева, 117
8(343) 374-30-15, uksap@mail.ru, www.uksap.ru
ИНН 6660008039; КПП 667001001

УТВЕРЖДАЮ
Директор
_____ О.В.Бурганова
«20» _____ 2015 г.
Приказ о введении в действие
№ 114/о от «20» _____ 2015 г.

ПОЛОЖЕНИЕ

по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных «УКСАП – ПД» государственного автономного образовательного учреждения среднего профессионального образования Свердловской области «Уральский колледж строительства, архитектуры и предпринимательства»

Одобрено и принято на Совете колледжа
Протокол № 32 от «13» октября 2015 г.
Председатель Совета колледжа
_____ В.А. Коновалов

Екатеринбург, 2015 г.

1. Общие положения.

1.1. Данное «Положение по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Положение) разработано в соответствии с Законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и другими нормативными правовыми актами и нормативными методическими документами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных.

1.2. Положение определяет порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ИСПДн, порядок проверки электронного журнала обращений к ИСПДн, 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 ИСПДн, порядок охраны и допуска посторонних лиц в защищаемые помещения.

2. Антивирусная защита

Настоящие правила определяют требования к организации защиты объекта ИСПДн от разрушающего воздействия вредоносного программного обеспечения (ПО), компьютерных вирусов и устанавливает ответственность руководителя и работников, эксплуатирующих и сопровождающих компьютеры в составе ИСПДн, за их выполнение. Настоящее положение распространяется на все объекты ИСПДн государственного автономного образовательного учреждения среднего профессионального образования Свердловской области «Уральский колледж строительства, архитектуры и предпринимательства» (далее - Колледж).

К использованию на компьютерах допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором безопасности.

Администратор безопасности осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.

Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы.

Еженедельно в начале работы, после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров.

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.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Настройки средств антивирусной защиты должны быть выполнены в соответствии с требованиями безопасности персональных данных определенного для данной ИСПДн

класса. Настройку средств антивирусной защиты выполняет администратор безопасности.

Файлы, помещаемые в электронный архив на магнитных носителях, 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, администратором безопасности должна быть выполнена антивирусная проверка ИСПДн.

На компьютеры запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

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 самостоятельно (или вместе с администратором безопасности) должен провести внеочередной антивирусный контроль компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить обработку данных в ИСПДн;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на ответственного за защиту информации.

Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на администратора безопасности и всех пользователей данной ИСПДн.

3. Защита информационной системы, ее средств и систем связи, и передача данных

В информационной системе должно быть обеспечено разделение функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации (функций безопасности) и функциональных возможностей пользователей по обработке информации.

Функциональные возможности по управлению (администрированию) информационной системой и управлению (администрированию) системой защиты информации включают функции по управлению базами данных, прикладным программным обеспечением, телекоммуникационным оборудованием, рабочими станциями, серверами, средствами защиты информации и иные функции, требующие высоких привилегий.

Разделение функциональных возможностей обеспечивается на физическом и (или) логическом уровне путем выделения части программно-технических средств информационной системы, реализующих функциональные возможности по управлению (администрированию) информационной системой и управлению (администрированию) системой защиты информации, в отдельный домен, использования различных автоматизированных рабочих мест и серверов, различных типов операционных систем, разных способов аутентификации, различных сетевых адресов, выделенных каналов управления и (или) комбинаций данных способов, а также иными методами.

В информационной системе должно обеспечиваться выделение автоматизированных рабочих мест для администраторов безопасности.

Защита информации при передачи ее (информации) по каналам связи, имеющим выход за пределы контролируемой зоны обеспечивается путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации.

В информационной системе осуществляется запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств, в том числе путем сигнализации, индикации.

Запрет несанкционированной удаленной активации осуществляется в отношении всех периферийных устройств ввода (вывода) информации, которые имеют возможность управления (запуска, включения, выключения) через компоненты программного обеспечение, установленные на рабочем месте пользователя, коммуникационных сервисов сторонних лиц (провайдеров) (ICQ, Skype и иные сервисы).

Запрет несанкционированной удаленной активации осуществляется через физическое исключение такой возможности и (или) путем управления программным обеспечением.

В исключительных случаях для решения установленных отдельных задач, решаемых информационной системой, допускается возможность удаленной активации периферийных устройств. При этом должно быть обеспечено определение и фиксирование в организационно-распорядительных документах по защите информации (документирование) перечня периферийных устройств, для которых допускается возможность удаленной активации и обеспечен контроль за активацией таких устройств.

В информационной системе должна обеспечиваться возможность физического отключения периферийных устройств (например, отключение при организации и проведении совещаний в помещениях, где размещены видеокамеры и микрофоны).

Должен осуществляться контроль санкционированного и исключение несанкционированного использования технологий мобильного кода (активного контента) в информационной системе, в том числе регистрация событий, связанных с использованием технологии мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологии мобильного кода. Технология мобильного кода включает, в том числе использование Java, JavaScript, ActiveX, PDF, Postscript, Flash-анимация и VBScript и иных технологий.

При контроле использования технологий мобильного кода должно быть обеспечено: определение перечня мобильного кода и технологий мобильного кода разрешенных и (или) запрещенных для использования в информационной системе; определение разрешенных мест распространения (серверы информационной системы) и использования мобильного кода (автоматизированные рабочие места, мобильные технические средства информационной системы) и функций информационной системы, для которых необходимо применение технологии мобильного кода; регистрация и анализ событий, связанных с разработкой, приобретением или внедрением технологии мобильного кода; исключение возможности использования запрещенного мобильного кода в информационной системе, а также внедрение мобильного кода в местах, не разрешенных для его установки.

В информационной системе должны быть реализованы механизмы обнаружения и анализа мобильного кода для выявления фактов несанкционированного использования мобильного кода и выполнения действий по реагированию (оповещение администраторов, изоляция мобильного кода (перемещение в карантин), блокирование мобильного кода, удаление мобильного кода) и иные действия.

Допустимо использование в информационной системе технологий (сервисов) передачи речи, необходимых для достижения целей обработки персональных данных.

Категории пользователей, которым разрешены разработка, приобретение или внедрение технологий передачи речи определяются матрицей доступа.

Технология передачи речи включает, в том числе, передачу речи через Интернет (в частности VoIP).

Допустимо использование в информационной системе технологий (сервисов) передачи видеоинформации, необходимых для достижения целей обработки персональных данных.

Категории пользователей, которым разрешены разработка, приобретение или внедрение технологий передачи речи определяются матрицей доступа. Технология передачи видеоинформации включает, в том числе, применение технологий видеоконференцсвязи.

В информационной системе осуществляется обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов (защита от атак типа «человек посередине»).

Для подтверждения подлинности сторон сетевого соединения (сеанса взаимодействия) и защиты сетевых устройств и сервисов от подмены осуществляется их аутентификация в соответствии с ИАФ.2 и ЗИС.10.

Контроль целостности передаваемой информации включает проверку целостности передаваемых пакетов (в частности в соответствии с ЗИС.3).

В информационной системе обеспечивается признание идентификатора сеанса связи недействительным после окончания сетевого соединения.

Должно обеспечиваться исключение возможности отрицания пользователем факта отправки информации другому пользователю.

Для исключения возможности отрицания пользователем факта отправки информации другому пользователю должны осуществляться: определение объектов или типов информации, для которых требуется обеспечение неотказуемости отправки (например, сообщения электронной почты); обеспечение целостности информации при ее подготовке к передаче и непосредственной ее передаче по каналам связи в соответствии с ЗИС.3; регистрация событий, связанных с отправкой информации другому пользователю в соответствии с РСБ.2.

Должно обеспечиваться исключение возможности отрицания пользователем факта получения информации от другого пользователя.

Для исключения возможности отрицания пользователем факта получения информации должны осуществляться: определение объектов или типов информации, для которых требуется обеспечение неотказуемости получения (сообщения электронной почты); обеспечение целостности полученной информации в соответствии с ЗИС.3; регистрация событий, связанных с получением информации от другого пользователя в соответствии с РСБ.2.

В информационной системе обеспечивается защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения, иных данных, не подлежащих изменению в процессе обработки информации.

Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации, обеспечивается принятием мер защиты информации, определенных в соответствии с настоящим документом, направленных на обеспечение их конфиденциальности и целостности.

Защита данных, не подлежащих изменению в процессе обработки информации, обеспечивается в отношении информации, хранящейся на жестких магнитных дисках, дисковых накопителях и иных накопителях в информационной системе.

При сегментировании информационной системы должна быть обеспечена защита периметров сегментов информационной системы в соответствии с УПД.3 и ЗИС.23.

Защита от угроз безопасности информации, направленных на отказ в обслуживании, осуществляется посредством реализации в информационной системе мер защиты информационной системы в соответствии с ЗИС.23 и повышенными характеристиками производительности телекоммуникационного оборудования и каналов передачи совместно с резервированием информации и технических средств, программного обеспечения, каналов передачи информации в соответствии с ОДТ.2, ОДТ.4 и ОДТ.5.

Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, основывается на:

- управлении (контроле) входящими в информационную систему и исходящими из информационной системы информационными потоками на физической и (или) логической границе информационной системы (сегментов информационной системы);
- обеспечении взаимодействия информационной системы и (или) ее сегментов с иными информационными системами и сетями только через сетевые интерфейсы, которые обеспечивают управление (контроль) информационными потоками с использованием средств защиты информации (управляемые (контролируемые) сетевые интерфейсы), установленных на физическом и (или) логическом периметре информационной системы или ее отдельных сегментов (маршрутизаторов, межсетевых экранов, коммутаторов, прокси-серверов, шлюзов безопасности, средств построения виртуальных частных сетей и иных средств защиты информации).

В информационной системе должна быть обеспечена возможность размещения публичных общедоступных ресурсов (в частности общедоступный веб-сервер), взаимодействующих с информационной системой через отдельные физические управляемые (контролируемые) сетевые интерфейсы.

В информационной системе должно быть обеспечено предоставление доступа во внутренние сегменты информационной системы (демилитаризованную зону) из внешних информационных систем и сетей только через средства защиты периметра (за исключением внутренних сегментов, которые специально выделены для такого взаимодействия).

Необходимо ограничить количество точек доступа в информационную систему из внешних информационных систем и сетей до минимально необходимого числа для решения постановленных задач, а также обеспечивающего постоянный и всесторонний контроль входящих и исходящих информационных потоков.

В информационной системе:

- должен быть исключен выход (вход) через управляемые (контролируемые) сетевые интерфейсы информационных потоков по умолчанию (реализация принципа «запрещено все, что не разрешено»);
- должен применяться отдельный физический управляемый (контролируемый) сетевой интерфейс для каждого внешнего телекоммуникационного сервиса;
- должны быть установлены правила управления информационными потоками для каждого физического управляемого (контролируемого) сетевого интерфейса;
- должна обеспечиваться защита информации при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны (при необходимости), путем применения организационно-технических мер или криптографических методов в соответствии с законодательством Российской Федерации.

Сетевые соединения должны блокироваться по мере их завершении и (или) по истечении 30 минут после прекращения активности.

Защита мобильных технических средств включает:

- реализацию в зависимости от мобильного технического средства (типа мобильного технического средства) мер по идентификации и аутентификации в соответствии с ИАФ.1 и ИАФ.5, управлению доступом в соответствии с УПД.2,

УПД.5, УПД.13 и УПД.15, ограничению программной среды в соответствии с ОПС.3, защите машинных носителей информации в соответствии с ЗНИ.1, ЗНИ.2, ЗНИ.4, ЗНИ.8, регистрации событий безопасности в соответствии с РСБ.1, РСБ.2, РСБ.3 и РСБ.5, антивирусной защите в соответствии с АВЗ.1 и АВЗ.2, контролю (анализу) защищенности в соответствии с АНЗ.1, АНЗ.2 и АНЗ.3, обеспечению целостности в соответствии с ОЦЛ.1;

- очистку (удаление) информации в мобильном техническом средстве после завершения сеанса удаленного доступа к защищаемой информации или принятие иных мер, исключающих несанкционированный доступ к хранимой защищаемой информации;
- уничтожение съемных машинных носителей информации, которые не подлежат очистке;
- выборочные проверки мобильных технических средств (на предмет их наличия) и хранящейся на них информации (например, на предмет отсутствия информации, не соответствующей маркировке носителя информации);
- запрет возможности автоматического запуска (без команды пользователя) в информационной системе программного обеспечения на мобильных технических средствах.

В информационной системе обеспечивается возможность подтверждения происхождения источника и целостности информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам, в том числе с использованием DNS-серверов. Подтверждение происхождения источника обеспечиваться путем:

- аутентификации в соответствии с ИАФ.7 и (или) ИАФ.2 сервера, являющегося источником ответов на запросы (сервер доменных имен или DNS-сервер) по определению сетевых адресов (IP-адресов) по сетевым именам (доменные имена);
- аутентификации в соответствии с ИАФ.7 и (или) ИАФ.2 сервера, являющегося источником ответов на запросы (кэширующий DNS-сервер) по определению сетевых имен (доменных имен) по сетевым адресам (IP-адресам).

4. Защита машинных носителей

Ответственность за организацию учета и использования машинных носителей данных, предназначенных для обработки и хранения персональных данных, возлагается на администратора защиты.

К машинным носителям информации относятся:

- магнитные ленты в кассетах;
- съемные носителя информации всех видов и способов подключения;
- несъемные жесткие магнитные диски.

Учёт машинных носителей информации осуществляется в соответствии с формой учетной документации.

Все машинные носители данных, используемые при работе со средствами вычислительной техники (СВТ) для обработки и хранения персональных данных, должны обязательно регистрироваться и учитываться. Допускается автоматизированный учет машинных носителей информации.

При обработке персональных данных на СВТ должен соблюдаться следующий общий порядок учета, хранения и уничтожения машинных носителей данных:

- Учет машинных носителей данных, предназначенных для записи персональных данных производится в Журнале учета машинных носителей информации.
- Каждому носителю информации присваивается учетный номер, который состоит из кода машинного носителя, номера объекта и порядкового номера по Журналу

учета машинных носителей информации.

- Учетный номер и гриф «конфиденциально» наносятся на носитель информации или его корпус. Если невозможно маркировать непосредственно машинный носитель данных, то маркируется упаковка, в которой хранится носитель. В этом случае учетный номер записывается также на носитель машинным способом.
- Хранение их должно осуществляться в условиях, исключающих возможность хищения, приведения в негодность или уничтожения содержащейся на них информации.
- Машинные носители данных после стирания с них персональных данных, с учета не снимаются, а хранятся наравне с другими машинными носителями.
- В последующем эти носители используются для записи персональных данных. Если носители не пригодны для дальнейшего использования, они подлежат уничтожению по соответствующему акту.
- О фактах утраты машинных носителей с грифом «конфиденциально» незамедлительно докладывается руководству и администратору защиты, проводится служебное расследование.
- Машинные носители данных должны пересылаться, по возможности, в металлических коробках, помещаемых в пакет, в упаковках, конвертах тем же порядком, что и конфиденциальные документы. На пакетах, упаковках, конвертах с носителями делается надпись: «Осторожно, машинные носители информации. Не прошивать».
- Машинные носители данных выдаются операторам или другим лицам, участвующим в обработке информации, для работы под расписку в Журнале учета машинных носителей информации. По завершению работы машинные носители данных сдаются ответственному (руководителю подразделения за их хранение.
- Копирование информации, содержащей персональные данные, с машинных носителей производится с разрешения руководства Колледжа по заявке руководителя отдела.
- Машинные носители с персональными данными, утратившими практическое значение или пришедшие в негодность, уничтожаются по соответствующему акту.

При подготовке документов должны соблюдаться следующие особенности учета, хранения и уничтожения машинных носителей данных:

- Машинные носители данных, предназначенные для записи персональных данных, выдаются работникам по письменному разрешению руководства Колледжа в необходимом для работы количестве под расписку в Журнале учета машинных носителей информации.
- Несъемные жесткие магнитные диски закрепляются за работником, ответственным за СВТ, в котором они установлены.
- В случае повреждения машинных носителей данных, содержащих персональные данные, работник, в пользовании которого они находятся, обязан сообщить о случившемся администратору защиты.
- В случае необходимости (командировка, отпуск и т. д.) машинные носители с персональными данными, сдаются работником ответственному лицу на постоянное или временное хранение в опечатанном виде. При этом на упаковке указывается срок их хранения, заверенный личной подписью работника. По истечению указанного срока информация может быть уничтожена, а носители могут повторно использоваться.
- Копирование персональных данных, с машинных носителей с целью передачи другим работникам производится с разрешения начальника отдела.

- Копирование осуществляется только на тех СВТ, на которых разрешена обработка персональных данных, и только на те носители, которые соответствуют грифу «конфиденциально».
- Передача скопированной информации третьим лицам производится по письменному разрешению руководства Колледжа.
- Хранящиеся на магнитных носителях и потерявшие актуальность персональные данные должны своевременно стираться (уничтожаться). Ответственность за это несет владелец информации.
- Начальник отдела не реже одного раза в год создает комиссию по проверке наличия и условий хранения персональных данных.
- Необходимо обеспечить маркировку машинных носителей информации (технических средств), дополнительно включающая:
- Информацию о возможности использования машинного носителя информации вне информационной системы.

Доступ к машинным носителям информации осуществляется только определенными должностными лицами, определяемым должностными обязанностями

В информационной системе должен осуществляться контроль использования интерфейсов ввода (вывода).

Контроль использования (разрешение или запрет) интерфейсов ввода (вывода) должен предусматривать: определение интерфейсов средств вычислительной техники, которые могут использоваться для ввода (вывода) информации, разрешенных и (или) запрещенных к использованию в информационной системе; определение категорий пользователей, которым предоставлен доступ к разрешенным к использованию интерфейсов ввода (вывода); принятие мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода); контроль доступа пользователей к разрешенным к использованию интерфейсов ввода (вывода).

В качестве мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода), должны применяться: опечатывание интерфейсов ввода (вывода); использование механических запирающих устройств; удаление драйверов, обеспечивающих работу интерфейсов ввода (вывода); применение средств защиты информации, обеспечивающих контроль использования интерфейсов ввода (вывода).

Стирание должно производиться по технологии, предусмотренной для данного типа носителя, с применением сертифицированных средств гарантированного уничтожения информации (допускается задействовать механизмы затирания встроенные в сертифицированные средства защиты информации).

Уничтожение носителей производится путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации (перед уничтожением, если носитель исправен, должно быть произведено гарантирование стирание информации на носителе). Непосредственные действия по уничтожению конкретного типа носителя должны быть достаточны для исключения возможности восстановления информации.

Бумажные и прочие сгораемые носители (конверты с неиспользуемыми более паролями) уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

По факту уничтожения или стирания носителей составляется акт, в журналах учета делаются соответствующие записи.

Процедуры стирания и уничтожения осуществляются комиссией, в которую входят: ответственный за эксплуатацию ИСПДн, ответственный за защиту информации, администратор безопасности.

В ИС должны быть обеспечены регистрация и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации;

Должны применяться следующие меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации:

- очистка всего физического пространства машинного носителя информации, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя.

Необходимо обеспечить исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах.

Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах должно предусматривать: определение типов машинных носителей информации, подлежащих хранению в помещениях, специально предназначенных для хранения машинных носителей информации (хранилище машинных носителей информации); физический контроль и хранение машинных носителей информации в помещениях, специально предназначенных для хранения машинных носителей информации (хранилище машинных носителей информации); защита машинных носителей информации до уничтожения (стирания) с них данных и остаточной информации (информации, которую можно восстановить после удаления с помощью нештатных средств и методов) с использованием средств стирания данных и остаточной информации.

5. Защита технических средств

Контролируемая зона включает пространство (территорию, здание, часть здания), в котором исключено неконтролируемое пребывание работников оператора и лиц, не имеющих постоянного допуска на объекты информационной системы (не являющихся работниками оператора), а также транспортных, технических и иных материальных средств.

Границами контролируемой зоны могут являться периметр охраняемой территории. Границы контролируемой зоны устанавливаются в Приказе об определении границ контролируемой зоны.

Контроль и управление физическим доступом предусматривает:

- определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
- санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
- ведение журнала физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

В качестве устройств вывода (отображения) информации в информационной системе рассматриваются экраны мониторов автоматизированных рабочих мест пользователей, мониторы консолей управления технических средств (серверов, телекоммуникационного оборудования и иных технических средств), видеопанели, видеостены и другие средства визуального отображения защищаемой информации, печатающие устройства (принтеры, плоттеры и иные устройства), аудиоустройства, многофункциональные устройства.

Размещение устройств вывода (отображения, печати) информации исключает возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Не следует размещать устройства вывода (отображения, печати) информации напротив оконных

проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.

6. Идентификация и аутентификация субъектов доступа к объектам доступа

При доступе в информационную систему должна осуществляться идентификация и аутентификация пользователей, являющихся работниками Колледжа (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

К внутренним пользователям в целях настоящего документа, относятся должностные лица Колледжа (пользователи, администраторы), выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств информационной системы в соответствии с должностными регламентами (инструкциями), утвержденными Колледжа, и которым в информационной системе присвоены учётные записи.

В качестве внутренних пользователей дополнительно рассматриваются должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной информационной системы, а также лица, привлекаемые на договорной основе для обеспечения функционирования информационной системы (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами оператора и которым в информационной системе также присвоены учетные записи.

Пользователи информационной системы должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации.

Аутентификация пользователя осуществляется с использованием паролей, аппаратных средств, биометрических характеристик, иных средств или в случае многофакторной (двухфакторной) аутентификации – определенной комбинации указанных средств.

В информационной системе должна быть обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

При удаленном доступе в систему с правами привилегированных учетных записей (администраторов) с использованием сети связи общего пользования, в том числе сети Интернет должна обеспечиваться многофакторная (двухфакторная) аутентификация.

При удаленном доступе в систему с правами непривилегированных учетных записей (пользователей) с использованием сети связи общего пользования, в том числе сети Интернет должна обеспечиваться многофакторная (двухфакторная) аутентификация.

В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа в систему с правами привилегированных учетных записей (администраторов).

Перечень устройств, используемых в информационной системе и подлежащих идентификации и аутентификации определен в Техническом паспорте.

Идентификация устройств в информационной системе обеспечивается по логическим именам (имя устройства и ID).

Аутентификация устройств в информационной системе обеспечивается с использованием соответствующих протоколов аутентификации.

С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации в ИСПДн руководителем назначается администратор безопасности; с целью контроля выполнения необходимых мероприятий по обеспечению безопасности ответственный за защиту информации.

Процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой ответственного за эксплуатацию данной ИСПДн. Форма заявки приведена ниже.

В заявке указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя ИСПДн, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИСПДн ранее зарегистрированного пользователя);
- должность (с полным наименованием отдела), фамилия, имя и отчество работника;
- имя пользователя (учетной записи) данного работника;
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИСПДн).

Заявку рассматривает руководитель, визируя её, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного работника к необходимым для решения им указанных в заявке задач ресурсам ИСПДн. Затем подписывает задание администратору защиты на внесение необходимых изменений в списки пользователей соответствующих подсистем ИСПДн.

На основании задания, в соответствии с документацией на средства защиты от несанкционированного доступа, администратор защиты производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля (возможно также регистрацию персонального идентификатора), заявленных прав доступа к ресурсам ИСПДн и другие необходимые действия, указанные в задании. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в течение 360 дней.

После внесения изменений в списки пользователей администратор защиты должен обеспечить настройки средств защиты соответствующие требованиям безопасности указанной ИСПДн. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания за подписью исполнителя – администратор защиты.

Работнику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации) и начальное (-ые) значение (-ия) пароля (-ей), которое (-ые) он обязан сменить при первом же входе в систему.

Исполненные заявка и задание (за подписью администратора защиты) передаются руководителю на хранение.

Они могут впоследствии использоваться:

- для восстановления полномочий пользователей после аварий ИСПДн;
- для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИСПДн при разборе конфликтных ситуаций;
- для проверки работниками контролирующих органов правильности настройки средств разграничения доступа к ресурсам ИСПДн.

При изменении идентификатора, новый идентификатор должен отличаться от старого минимум на 3 позиции, повторное использование идентификатора запрещено в течение всего периода эксплуатации информационной системы.

Ответственным за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятия мер в случае утраты и (или) компрометации средств аутентификации является администратор безопасности.

Личные пароли должны генерироваться и распределяться централизованно.

В числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т. п.).

Символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры.

Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т. д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т. п.).

Изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информации информационной системы; выдача средств аутентификации пользователям; генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации); установление характеристик пароля (при использовании в информационной системе механизмов аутентификации на основе пароля); блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации; назначение необходимых характеристик средств аутентификации (в том числе механизма пароля); обновление аутентификационной информации (замена средств аутентификации); защита аутентификационной информации от неправомерных доступа к ней и модифицирования реализуется средствами СЗИ.

Вводимые символы аутентификационной информации должны отображаться условными знаками «*», «.» или иными знаками.

В случае необходимости предоставления прав доступа к ресурсам информационной системы работнику сторонней организации (не являющимся работником Колледжа) руководитель структурного подразделения где возникла такая необходимость, становится куратором работ по предоставлению прав доступа и имеет полную ответственность за предоставленные права доступа и использование ресурсов информационной системы работником сторонней организации.

Предоставление прав доступа к ресурсам информационной системы работнику сторонней организации происходит аналогично процедуре предоставления прав доступа к ресурсам информационной системы работнику Колледжа.

7. Контроль (анализ) защищенности информации

Выявление (поиск), анализ и устранение уязвимостей в информационной системе включает в себя:

- выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;
- разработку по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;
- анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;
- устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;
- информирование должностных лиц оператора (пользователей, администраторов, подразделения по защите информации) о результатах поиска уязвимостей и

оценки достаточности реализованных мер защиты информации.

Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и эксплуатации информационной системы.

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 информационной системы), направленные на устранение возможности использования выявленных уязвимостей.

Необходимо использовать для выявления (поиска) уязвимостей средств анализа (контроля) защищенности (сканеров безопасности), имеющих стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования информационной системы на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей.

Необходимо уточнять перечень сканируемых в информационной системе уязвимостей с установленной им периодичностью, а также после появления информации о новых уязвимостях.

Доступ к функциям выявления (поиска) уязвимостей предоставляется только администраторам (предоставление такой возможности только администраторам безопасности).

Настоящие правила регламентируют обеспечение безопасности информации при проведении обновлении, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн.

Все изменения конфигураций технических и программных средств ИСПДн должны производиться только на основании заявок ответственного за эксплуатацию конкретной ИСПДн.

Право внесения изменений в конфигурацию аппаратно-программных средств защищенных ИСПДн предоставляется:

- в отношении системных и прикладных программных средств – администратору защиты по согласованию (в случае, если проводилась аттестация) с органом по аттестации, проводившим аттестацию данной ИСПДн;
- в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты – администратору защиты по согласованию (в случае, если проводилась аттестация) с органом по аттестации, проводившим аттестацию данной ИСПДн.

Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме вышеперечисленных уполномоченных работников и подразделений, запрещено.

Процедура внесения изменений в конфигурацию системных и прикладных программных средств ИСПДн, а также средств защиты информации инициируется заявкой ответственного за эксплуатацию ИСПДн.

В заявке могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств ИСПДн:

- установка (развертывание) на компьютер(ы) программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной ИСПДн;
- обновление (замена) на компьютере(ах) программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения

определенной задачи программ);
- изменение настроек средств защиты информации;
- удаление с компьютера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данном компьютере).

Также в заявке указывается условное наименование ИСПДн. Наименования задач указываются в соответствии с перечнем задач архива дистрибутивов установленного программного обеспечения, которые можно решать с использованием указанного компьютера.

Заявку ответственного за эксплуатацию ИСПДн, в которой требуется произвести изменения конфигурации, рассматривает руководитель, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений.

После чего заявка передается администратору защиты для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера указанного в заявке ИСПДн.

Подготовка обновления, модификации общесистемного и прикладного программного обеспечения ИСПДн тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного программного обеспечения, внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов на компьютерах, (обновление) и удаление системных и прикладных программных средств производится администратором безопасности по согласованию с органом по аттестации (в случае, если проводилась аттестация), проводившим аттестацию данной ИСПДн. Работы производятся в присутствии ответственного за эксплуатацию данной ИСПДн.

Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

Установка и обновление ПО (системного, тестового и т. п.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных установленным порядком, прикладного ПО – с эталонных копий программных средств, полученных из архива дистрибутивов установленного программного обеспечения.

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

После установки (обновления) ПО, администратор защиты должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность ПО и правильность их настройки и произвести соответствующую запись в «Журнале учета нештатных ситуаций в ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн», делает отметку о выполнении (на обратной стороне заявки) и в «Техническом паспорте».

Формат записей «Журнала учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» устанавливается приказом руководителя Организации.

При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за ее эксплуатацию докладывает об этом ответственному за защиту информации, который в свою очередь связывается с работниками органа по аттестации (в случае, если проводилась аттестация) и в дальнейшем действует согласно их инструкций. В данном случае администратор защиты обязан предпринять необходимые меры для затирания защищаемой информации, которая

хранилась на дисках компьютера. Оригиналы заявок (документов), на основании которых производились изменения в составе программных средств компьютеров с отметками о внесении изменений в состав программных средств, должны храниться вместе с техническим паспортом на ИСПДн и «Журналом учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» у ответственного за защиту информации.

Копии заявок могут храниться у администратора защиты:

- для восстановления конфигурации ИСПДн после аварий;
- для контроля правомерности установки на ИСПДн средств для решения соответствующих задач при разборе конфликтных ситуаций;
- для проверки правильности установки и настройки средств защиты ИСПДн

Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью администратора защиты и работника ответственного за эксплуатацию данной ИСПДн.

Данный раздел Положения определяет порядок контроля соблюдения условий использования средств защиты информации (далее – СЗИ).

Технические средства защиты информации являются важным компонентом ОБ ПДн.

Порядок работы с техническими СЗИ определен в соответствующих руководствах по настройке и использованию СЗИ обязательных для исполнения, как работниками обрабатывающими конфиденциальную информацию, так и администратором безопасности ИСПДн.

Право проверки соблюдения условий использования средств защиты информации имеют:

- руководитель;
- ответственный за защиту информации;
- администратор безопасности.

Пользователю ИСПДн категорически запрещается:

- обрабатывать конфиденциальную информацию с отключенными СЗИ;
- менять настройки СЗИ.

Администратору безопасности запрещается менять настройки программно-аппаратных СЗИ предустановленные специалистом организации, имеющей лицензию на деятельность по технической защите информации, без согласования с этой организацией.

В информационной системе должны обеспечиваться регистрация событий и оповещение (сигнализация, индикация) администратора безопасности о событиях, связанных с нарушением работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации.

Криптографические средства защиты информации должны использоваться в соответствии с технической и эксплуатационной документацией на них, а также в соответствии с правилами пользования ими.

В информационной системе должны обеспечиваться регистрация событий и оповещение (сигнализация, индикация) администратора безопасности о событиях, связанных с нарушением работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации.

При контроле состава технических средств, программного обеспечения и средств защиты информации осуществляется:

- контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации информационной системы и принятие мер, направленных на устранение выявленных недостатков;
- контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей

(актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;

- контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;
- исключение (восстановление) из состава информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

В информационной системе должна обеспечиваться регистрация событий безопасности, связанных с изменением состава технических средств, программного обеспечения и средств защиты информации.

При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе осуществляется:

- контроль правил генерации и смены паролей пользователей в соответствии с ИАФ.1 и ИАФ.4;
- контроль заведения и удаления учетных записей пользователей в соответствии с УПД.1;
- контроль реализации правил разграничения доступом в соответствии с УПД.2;
- контроль реализации полномочий пользователей в соответствии с УПД.4 и УПД.5;
- контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей, предусмотренных организационно-распорядительными документами по защите информации оператора;
- устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

В информационной системе должна обеспечиваться регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступом и полномочий пользователей.

В информационной системе должна обеспечиваться регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступом и полномочий пользователей.

8. Обеспечение доступности информации

Должен осуществляться контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование.

Контроль безотказного функционирования проводится в отношении серверного и телекоммуникационного оборудования, каналов связи, средств обеспечения функционирования информационной системы путем периодической проверки работоспособности в соответствии с эксплуатационной документацией (в том числе путем посылки тестовых сообщений и принятия «ответов», визуального контроля, контроля трафика, контроля «поведения» системы или иными методами).

При обнаружении отказов функционирования осуществляется их локализация и принятие мер по восстановлению отказавших средств в соответствии с ОЦЛ.3, их тестирование в соответствии с эксплуатационной документацией, а также регистрация событий, связанных с отказами функционирования, в соответствующих журналах.

Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

К использованию, для создания резервной копии в ИСПДн, допускаются только зарегистрированные в журнале учета носители.

Администратор безопасности обязан осуществлять периодическое резервное копирование конфиденциальной информации.

Еженедельно, по окончанию работы с конфиденциальными документами (содержащими персональные данные) на компьютере, пользователь, при отсутствии администратора, обязан создавать резервную копию конфиденциальных документов на зарегистрированный носитель (ЖМД, ГМД, CD, DVD-диски, USB накопитель, другие), создавая тем самым резервный электронный архив конфиденциальных документов.

Носители информации (ЖМД, ГМД, CD-ROM, USB накопитель, другие), предназначенные для создания резервной копии и хранения конфиденциальной информации выдаются установленным порядком руководителем, ответственным за защиту информации и(или) администратором. По окончании процедуры резервного копирования электронные носители конфиденциальной информации сдаются на хранение администратору безопасности, или руководителю, или ответственному за защиту информации.

Перед резервным копированием пользователь или администратор безопасности обязан проверить электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель) на отсутствие вирусов.

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль в соответствии с п. 7 настоящего Положения.

Запрещается запись посторонней информации на электронные носители (ЖМД, ГМД, CD-ROM, USB накопитель и другие) резервной копии.

Порядок создания резервной копии:

- вставить в компьютер зарегистрированный электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель, другие) для резервного копирования;
- выбрать необходимый каталог (файл) для создания резервного архива;
- при использовании систем управления базами данных необходимо создать файл с резервной копией защищаемой информации с помощью встроенных средств системы;
- выполнить процедуру создания резервной копии;
- произвести копирование на отчуждаемый носитель;
- произвести отключение отчуждаемого носителя и, создав не обходимые записи в журналах убрать носитель в хранилище.

Хранение отчуждаемого носителя с резервной копией защищаемой информации осуществляется в специальном металлическом хранилище совместно с ключевой и аутентифицирующей информацией.

При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется администратором безопасности в специальном хранилище.

При необходимости ремонта технических средств, с них удаляются опечатывающие пломбы и по согласованию с администратором безопасности, ответственным за защиту информации и, при условии проведенной аттестации информационной системы, представителем организации, проводившей аттестацию, оборудование передается в сервисный центр производителя. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению в

соответствии с порядком уничтожения носителей защищаемой информации. Работа с использованием неисправных технических средств запрещается.

При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания, с целью предотвращения повреждения технических средств и(или) защищаемой информации в результате сбоев в сети электропитания.

При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных. Настройку данных средств должен выполнять работник организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся в хранилище. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный носитель.

Ответственность за проведение резервного копирования в ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора безопасности.

Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения баз данных возлагается на администратора безопасности.

Ответственность за проведение мероприятий по восстановлению средств защиты информации (далее – СЗИ) возлагается администратора безопасности.

Должна осуществляться с установленной периодичностью проверка работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий (периодичность проверки работоспособности определяется оператором).

Должно осуществляться хранение (размещение) резервных копий информации на отдельных (размещенных вне информационной системы) средствах хранения резервных копий и в помещениях, специально предназначенных для хранения резервных копий информации, которые исключают воздействие внешних факторов на хранимую информацию.

Необходимо обеспечить возможность восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала.

Восстановление информации с резервных машинных носителей информации (резервных копий) должно предусматривать: определение времени, в течение которого должно быть обеспечено восстановление информации и обеспечивающего требуемые условия непрерывности функционирования информационной системы и доступности информации; восстановление информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала; регистрация событий, связанных восстановлением информации с резервных машинных носителей информации.

Контроль состояния и качества предоставления уполномоченным лицом (провайдером) вычислительных ресурсов (мощностей), в том числе по передаче информации, предусматривает:

- контроль выполнения уполномоченным лицом требований о защите информации, установленных законодательством Российской Федерации и условиями договора (соглашения), на основании которого уполномоченное лицо обрабатывает информацию или предоставляет вычислительные ресурсы (мощности);
- мониторинг состояния и качества предоставления уполномоченным лицом (провайдером) вычислительных ресурсов (мощностей);

- мониторинг состояния и качества предоставления уполномоченным лицом (провайдером)услуг по передаче информации.

Резервированию подлежат технические средства, программное обеспечение, каналы передачи информации, средства обеспечения функционирования, непосредственно участвующие в обработке персональных данных.

Необходимо обеспечить наличие резервных источников питания (кратковременных и долговременным) серверам и рабочим местам, на которых производится обработка и хранение персональных данных, а также техническим средствам, отвечающим за передачу персональных данных по каналам связи.

9. Обеспечение целостности информационной системы и информации

Контроль целостности программного обеспечения включает в себя:

- контроль целостности программного обеспечения средств защиты информации, включая их обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам компонентов средств защиты информации в процессе загрузки и (или) динамически в процессе работы информационной системы;
- контроль целостности компонентов программного обеспечения (за исключением средств защиты информации), определяемого оператором исходя из возможности реализации угроз безопасности информации, по наличию имен (идентификаторов) компонентов программного обеспечения и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы информационной системы;
- контроль применения средств разработки и отладки программ в составе программного обеспечения информационной системы;
- тестирование с установленной периодичностью функций безопасности средств защиты информации, в том числе с помощью тест-программ, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств, в соответствии с АН3.1 и АН3.2;
- обеспечение физической защиты технических средств информационной системы в соответствии с ЗТС.2 и ЗТС.3.

В информационной системе контроль целостности средств защиты информации должен осуществляться по контрольным суммам всех компонентов средств защиты информации, как в процессе загрузки, так и динамически в процессе работы системы.

Должна быть исключена возможность использования средств разработки и отладки программ во время обработки и (или) хранения информации в целях обеспечения целостности программной среды.

Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

К использованию, для создания резервной копии в ИСПДн, допускаются только зарегистрированные в журнале учета носители.

Администратор безопасности обязан осуществлять периодическое резервное копирование конфиденциальной информации.

Еженедельно, по окончанию работы с конфиденциальными документами (содержащими персональные данные) на компьютере, пользователь, при отсутствии администратора, обязан создавать резервную копию конфиденциальных документов на зарегистрированный носитель (ЖМД, ГМД, CD, DVD – диски, USB накопитель, другие), создавая тем самым резервный электронный архив конфиденциальных документов.

Носители информации (ЖМД, ГМД, CD-ROM, USB накопитель, другие), предназначенные для создания резервной копии и хранения конфиденциальной информации выдаются установленным порядком руководителем, ответственным за защиту

информации и(или) администратором. По окончании процедуры резервного копирования электронные носители конфиденциальной информации сдаются на хранение администратору безопасности, или руководителю, или ответственному за защиту информации.

Перед резервным копированием пользователь или администратор безопасности обязан проверить электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель) на отсутствие вирусов.

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль;

Запрещается запись посторонней информации на электронные носители (ЖМД, ГМД, CD-ROM, USB накопитель и другие) резервной копии.

Порядок создания резервной копии:

- вставить в компьютер зарегистрированный электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель, другие) для резервного копирования;
- выбрать необходимый каталог (файл) для создания резервного архива;
- при использовании систем управления базами данных необходимо создать файл с резервной копией защищаемой информации с помощью встроенных средств системы;
- выполнить процедуру создания резервной копии;
- произвести копирование на отчуждаемый носитель;
- произвести отключение отчуждаемого носителя и, создав не обходимые записи в журналах убрать носитель в хранилище.

Хранение отчуждаемого носителя с резервной копией защищаемой информации осуществляется в специальном металлическом хранилище совместно с ключевой и аутентифицирующей информацией.

При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование зашищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется администратором безопасности в специальном хранилище.

При необходимости ремонта технических средств, с них удаляются опечатывающие пломбы и по согласованию с администратором безопасности, ответственным за защиту информации и, при условии проведенной аттестации информационной системы, представителем организации, проводившей аттестацию, оборудование передается в сервисный центр производителя. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению в соответствии с порядком уничтожения носителей защищаемой информации. Работа с использованием неисправных технических средств запрещается.

При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания, с целью предотвращения повреждения технических средств и(или) защищаемой информации в результате сбоев в сети электропитания.

При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных. Настройку данных средств должен выполнять работник организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся в хранилище. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный носитель.

Ответственность за проведение резервного копирования в ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора безопасности.

Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения баз данных возлагается на администратора безопасности.

Ответственность за проведение мероприятий по восстановлению средств защиты информации (далее – СЗИ) возлагается администратора безопасности.

Защита от спама реализуется на точках входа в информационную систему (выхода) информационных потоков (межсетевые экраны, почтовые серверы, Web-серверы, прокси-серверы и серверы удаленного доступа), а также на автоматизированных рабочих местах, серверах и (или) мобильных технических средствах, подключенных к сетям связи общего пользования, для обнаружения и реагирования на поступление по электронной почте незапрашиваемых электронных сообщений (писем, документов) или в приложениях к электронным письмам.

Защита от спама обеспечивается применением специализированных средств защиты, реализующих следующие механизмы защиты:

- фильтрация по содержимому электронных сообщений (писем, документов) с использованием критериев, позволяющих относить сообщения к спаму сигнатурным и (или) эвристическим методами;
- фильтрация на основе информации об отправителе электронного сообщения (в том числе с использованием «черных» списков(запрещенные отправители) и (или) «белых» списков (разрешенные отправители).
- должно осуществляться обновление базы «черных» («белых») списков и контроль целостности базы «черных» («белых») списков.

10. Обнаружение (предотвращение) вторжений

В целях обеспечения защиты ЛВС от деструктивных информационных воздействий осуществляется обнаружение и предотвращение сетевых атак на входе в ЛВС.

Защита от сетевых атак в ЛВС осуществляется средствами обнаружения и предотвращения сетевых атак, размещаемыми на входе в ЛВС. Обнаружение сетевых атак осуществляется путем анализа в режиме реального времени входящих в ЛВС и исходящих из нее информационных потоков на предмет выявления в них сигнатур известных атак. Управление средствами обнаружения и предотвращения сетевых атак осуществляется централизованно.

В информационной системе должно обеспечиваться централизованное управление (администрирование) компонентами системы обнаружения вторжений, установленными в различных сегментах информационной системы.

Базы данных сигнатур средств обнаружения и предотвращения сетевых атак регулярно централизованно обновляются, обеспечивается возможность редактирования базы решающих правил (добавление и (или) исключение решающих правил) со стороны администраторов безопасности для предотвращения определенных оператором компьютерных атак и (или) сокращения нагрузки на информационную систему, а также минимизации ложных срабатываний системы обнаружения вторжений, а также устанавливается порядок редактирования базы решающих правил. В случае редактирования базы решающих правил запись об этом событии с указанием произведенных изменений фиксируется в соответствующем журнале регистрации событий безопасности.

11. Ограничение программной среды

В информационной системе разрешен автоматический запуск компонентов программного обеспечения (файлов, объектов баз данных, хранимых процедур и иных компонентов), использование которых требуется для реализации информационной технологии информационной системы.

В информационной системе обеспечивается использование автоматизированных механизмов управления запуском (обращениями) компонентов программного обеспечения.

Допускается установка только тех компонентов программного обеспечения, использование которых требуется для реализации информационной технологии информационной системы. Настраиваемая конфигурация данных компонентов должна производится в соответствии с установленными правилами настройки.

В информационной системе обеспечивается использование средств автоматизации для применения и контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации.

Установка (инсталляция) в информационной системе программного обеспечения (вида, типа, класса программного обеспечения) и (или) его компонентов осуществляется с учетом перечня программного обеспечения и (или) его компонентов, разрешенных к установке, и (или) перечнем программного обеспечения и (или) его компонентов, запрещенных к установке («черный список»). Указанные перечни программного обеспечения и (или) его компонентов регламентированы Техническим паспортом ИСПДН.

Установка (инсталляция) в информационной системе программного обеспечения и (или) его компонентов должна осуществляться только от имени администратора в соответствии с УПД.5.

В информационной системе обеспечивается периодический контроль установленного (инсталлированного) в информационной системе программного обеспечения на предмет соответствия его перечню программного обеспечения, разрешенному к установке в информационной системе в соответствии с АНЗ.4, а также на предмет отсутствия программного обеспечения, запрещенного оператором к установке.

12. Регистрация событий безопасности

В информационной системе должно осуществляться реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти. Реагирование на сбои при регистрации событий безопасности должно предусматривать: предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности; реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов информационной системы, запись поверх устаревших хранимых записей событий безопасности.

В информационной системе должна обеспечиваться защита информации о событиях безопасности.

Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в соответствии с настоящим методическим документом, 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) должен предоставляться только уполномоченным должностным лицам.

В целях своевременного выявления нарушений ИБ в информационной системе осуществляется контроль событий ИБ операционных и прикладных систем, СУБД, сетевого оборудования и средств защиты.

В информационной системе осуществляется регистрация и учет в журналах событий операционных и прикладных систем, СУБД, сетевого оборудования и средств защиты, которые могут быть связаны с нарушениями ИБ.

В обязательном порядке подлежат регистрации:

- действия пользователей по доступу к операционным и прикладным системам;
- действия администраторов по изменению настроек средств обработки, хранения и передачи информации, средств защиты информации, прав доступа пользователей;
- попытки несанкционированного подключения к сетевой инфраструктуре и подмены адреса сетевых устройств;
- события, связанные с изменением привилегий учетных записей;
- попытки получения доступа к журналам событий.

Обеспечить хранение журналов учета событий в течение заданного периода времени. Предусматриваются механизмы защиты журналов учета событий от переполнения, несанкционированного просмотра и изменения.

Журналы событий регулярно анализируются работниками подразделения ИБ. Для повышения эффективности контроля применяются средства анализа и корреляции событий. В целях обеспечения возможности корреляции событий осуществляется синхронизация времени всех систем с единым доверенным источником.

Перечень событий, состав событий, подлежащих регистрации, период и условия хранения, периодичность контроля журналов, реагирование на сбои при регистрации событий безопасности, мониторинг результатов регистрации событий безопасности и реагирование на них, защита информации о событиях безопасности и другие меры безопасности определяются нормативными и организационно-распорядительными документами Колледжа.

Результаты регистрации и учета событий используются при проведении мероприятий по управлению инцидентами ИБ.

Необходимо обеспечить пересмотр перечня событий безопасности, подлежащих регистрации, не менее чем один раз в год, а также по результатам контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе.

В перечень событий безопасности, подлежащих регистрации, должны быть включены события, связанные с изменением привилегий учетных записей.

Обеспечить срок хранения информации о зарегистрированных событиях безопасности не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации, при этом осуществляется хранение только записей о выявленных событиях безопасности.

В информационной системе должны быть определены состав и содержание информации о событиях безопасности, подлежащих регистрации.

Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

При регистрации входа (выхода) субъектов доступа в информационную систему и загрузки (останова) операционной системы состав и содержание информации должны, как минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная),

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

При регистрации подключения машинных носителей информации и вывода информации на носители информации состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, 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).

При регистрации попыток удаленного доступа к информационной системе состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.

В информационной системе должна обеспечиваться запись дополнительной информации о событиях безопасности, включающую полнотекстовую запись привилегированных команд (команд, управляющих системными функциями).

В информационной системе должны осуществляться сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения информации о событиях безопасности.

Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должен предусматривать: возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности определенных в соответствии с РСБ.1; генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с РСБ.1 с составом и содержанием информации, определенными в соответствии с РСБ.2; хранение информации о событиях безопасности в течение времени, установленного в соответствии с РСБ.1.

Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с РСБ.1, составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с РСБ.2, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности в соответствии с РСБ.1.

В информационной системе должно быть обеспечено централизованное автоматизированное управление сбором, записью и хранением информации о событиях безопасности.

Необходимо осуществлять мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться для всех событий, подлежащих регистрации в соответствии с РСБ.1, и с установленной периодичностью, и обеспечивающей своевременное выявление признаков инцидентов безопасности в информационной системе.

В случае выявление признаков инцидентов безопасности в информационной системе осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

В информационной системе должно осуществляться генерирование надежных меток времени и (или) синхронизация системного времени.

Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в информационной системе достигается посредством применения внутренних системных часов информационной системы.

В информационной системе обеспечивается резервное копирование записей регистрации (аудита).

13. Управлением доступом субъектов доступа к объектам доступа

Определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей); объединение учетных записей в группы (при необходимости); верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя; заведение, активация, блокирование и уничтожение учетных записей пользователей; пересмотр и, при необходимости, корректировка учетных записей пользователей с периодичностью, определяемой оператором; порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов; оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях; уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе реализуется средствами СЗИ.

Предоставление пользователям прав доступа к объектам доступа информационной системы, осуществляется основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными системами.

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, работникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

Необходимо использовать автоматизированные средства поддержки управления учетными записями пользователей.

В информационной системе должно осуществляться автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования.

В информационной системе реализован дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка,

содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа.

Тип доступа включает операцию по чтению, записи, удалению, выполнению и другие операции.

Правила разграничения доступа реализуются на основе установленной матрицы доступа.

В информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов при входе в информационную систему.

В информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов к техническим средствам, устройствам, внешним устройствам.

В информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов к объектам, создаваемым общесистемным (общим) программным обеспечением.

Управление информационными потоками осуществляется на основании Схемы информационных потоков и должно обеспечивать разрешенный маршрут прохождения информации между пользователями, устройствами, сегментами в рамках информационной системы, а также между информационными системами или при взаимодействии с сетью Интернет (или другими информационно-телекоммуникационными сетями международного информационного обмена). Управление информационными потоками должно блокировать передачу защищаемой информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из информационной системы и (или) входящие в информационную систему.

Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы основывается на утвержденной Матрице доступа и реализуется средствами СЗИ.

Назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями осуществляется согласно должностных инструкций и обязанностей.

В информационной системе установлено ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) в соответствии с ИАФ.4, после чего происходит блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему (доступа к информационной системе).

В информационной системе обеспечивается блокирование сеанса доступа пользователя после времени бездействия (неактивности) пользователя.

Запрещены любые действия пользователей до идентификации и аутентификации.

Защита удаленного доступа пользователей к ресурсам информационной системы должна реализовываться сертифицированными средствами защиты информации.

Ограничение на использование удаленного доступа, предоставление удаленного доступа пользователям осуществляется на основании должностных обязанностей и в соответствии с УПД.2.

Администратор безопасности обязан проводить мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа информационной системы.

В информационной системе используется ограниченное (минимально необходимое) количество точек подключения к информационной системе при организации удаленного доступа к объектам доступа информационной системы.

В информационной системе исключается удаленный доступ от имени привилегированных учетных записей (администраторов) для администрирования информационной системы и ее системы защиты информации.

В информационной системе обеспечивается мониторинг и контроль удаленного доступа на предмет выявления установления несанкционированного соединения технических средств (устройств) с информационной системой.

Управление взаимодействием с внешними информационными системами регламентируется в Регламенте управления взаимодействием с информационными системами сторонних организаций, который включает в себя:

- определение типов прикладного программного обеспечения информационной системы, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних информационных систем;
- определение системных учетных записей, используемых в рамках данного взаимодействия;
- определение порядка предоставления доступа к информационной системе авторизованными (уполномоченным) пользователями из внешних информационных систем;
- определение порядка обработки, хранения и передачи информации с использованием внешних информационных систем.

Управление взаимодействием с внешними информационными системами в целях межведомственного электронного взаимодействия, исполнения государственных и муниципальных функций, формирования базовых государственных информационных ресурсов осуществляется в том числе с использованием единой системы идентификации и аутентификации, созданной в соответствии с постановлением Правительства Российской Федерации от 28 ноября 2011 г. № 977.

Доступ к информационной системе предоставляется авторизованным (уполномоченным) пользователям внешних информационных систем или разрешается обработка, хранение и передача информации с использованием внешней информационной системы при выполнении следующих условий:

- при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы;
- при наличии подтверждения выполнения во внешней информационной системе предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

Доверенная загрузка средств вычислительной техники обеспечивается путем установки специализированных средств защиты информации и (или) путем установки пароля на BIOS, опечатыванием системного блока специальными защитными пломбами, а также принятием других организационно-технических мер, направленных на:

- блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы;
- контроль доступа пользователей к процессу загрузки операционной системы;
- контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники.

В информационной системе применяется доверенная загрузка на разных уровнях (уровня базовой системы ввода-вывода, уровня платы расширения и уровня загрузочной записи).

В информационной системе должна осуществляться доверенная загрузка уровня базовой системы ввода-вывода или уровня платы расширения.

Под использованием мобильных технических устройств и носителей информации в ИС Колледжа понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и мобильными устройствами, а также носителями информации.

В ИС допускается использование только учтенных мобильных устройств и носителей информации, которые являются собственностью Колледжа и подвергаются регулярной ревизии и контролю.

На предоставленных Колледжем мобильных технических устройствах допускается использование коммерческого ПО, входящего в Реестр разрешенного к использованию ПО и указанного в Техническом паспорте.

К предоставленным Колледжем мобильным устройствам и носителям информации предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ИС).

Мобильные устройства и носители информации предоставляются работникам Колледжа по инициативе руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у работника Организации производственной необходимости.

Процесс предоставления работнику Организации мобильных устройств и носителей информации состоит из следующих этапов:

- подготовка заявки в утвержденной форме, осуществляется руководителем структурного подразделения на имя директора Колледжа;
- согласование подготовленной заявки (для получения заключения о возможности предоставления работнику Колледжа заявленного мобильного устройства и/или носителя информации) с начальником отдела ИТ;
- передача оригинала заявки в отдел ИТ для учета предоставленного мобильного устройства и/или носителя информации и внесения изменений в «Список работников Колледжа, имеющих право работы с мобильными устройствами», а также выполнения технических настроек по регистрации мобильного устройства в ИС и/или предоставлению права использования носителей информации на АРМах Колледжа (в случае согласования заявки).

Внос на территорию Колледжа предоставленных мобильных устройств работниками Колледжа, а также вынос их за его пределы производится только на основании «Списка работников Колледжа, имеющих право работы с мобильными устройствами», который ведется отделом ИТ на основании утвержденных заявок и передается в службу безопасности.

Внос на территорию Колледжа предоставленных мобильных устройств работниками подрядных и сторонних организаций, а также вынос их за его пределы производится на основании заполненной по форме заявки на внос/вынос мобильного устройства, подписанной Руководителем структурного подразделения.

При использовании предоставленных работникам Организации мобильных устройств и носителей информации необходимо:

- соблюдать требования настоящего Положения;
- использовать мобильные устройства и носители информации исключительно для выполнения своих служебных обязанностей;
- ставить в известность администраторов ИС о любых фактах нарушения требований настоящего Положения;
- бережно относится к мобильным устройствам и носителям информации;
- эксплуатировать и транспортировать мобильные устройства и носители информации в соответствии с требованиями производителей;

- обеспечивать физическую безопасность мобильных устройств и носителей информации всеми разумными способами;
- извещать администраторов ИС о фактах утраты (кражи) мобильных устройств и носителей информации.

При использовании предоставленных работникам Колледжа мобильных устройств и носителей информации запрещено:

- использовать мобильные устройства и носители информации в личных целях;
- передавать мобильные устройства и носители информации другим лицам (за исключением администраторов ИС);
- оставлять мобильные устройства и носители информации без присмотра, если не предприняты действия по обеспечению их физической безопасности.

Любое взаимодействие (обработка, прием/передача информации) инициированное работником Колледжа между ИС и неучтенными (личными) мобильными устройствами, а также носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с администраторами ИС заранее). Колледж оставляет за собой право блокировать или ограничивать использование таких устройств и носителей информации.

Информация об использовании работниками Колледжа мобильных устройств и носителей информации в ИС протоколируется и, при необходимости, может быть предоставлена руководителям структурных подразделений, а также руководству Колледжа.

При подозрении работника Колледжа в несанкционированном и/или нецелевом использовании мобильных устройств и носителей информации инициализируется служебная проверка, проводимая комиссией, состав которой определяется руководителем Колледжа.

По факту выясненных обстоятельств составляется акт расследования инцидента и передается Руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Колледжа и действующему законодательству. Акт расследования инцидента и сведения о принятых мерах подлежат передаче в отдел ИТ.

Информация, хранящаяся на предоставляемых Колледжу мобильных устройствах и носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

В случае увольнения или перевода работника в другое структурное подразделение Колледжа, предоставленные ему мобильные устройства и носители информации изымаются.

14. Управление конфигурацией информационной системы и системы защиты персональных данных

Лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных определяет ответственный за обеспечение безопасности персональных данных, на основании должностных обязанностей и требований.

Перед изменениями настроек и баз данных средств защиты информации должны быть созданы резервные копии данных средств.

В настоящем Положении регламентируются мероприятия по настройке компонент резервного копирования СЗИ, резервированию СЗИ, хранению носителей резервных копий, выводу из эксплуатации носителей резервных копий, восстановлению работоспособности СЗИ.

Имеются следующие типы резервных копий СЗИ:

Тип	Периодичность резервирования	Способ резервирования	Место хранения	Срок хранения
Первый тип	1 раз в день (в ночное время)	автоматически	на несъемных жестких магнитных дисках	30 суток
Второй тип	после каждой установки/переустановки СЗИ, а также после любого изменения конфигурации СЗИ	вручную	на однократно записываемые оптические компакт-диски	5 недель
Третий тип	1 раз в месяц (в первый рабочий день месяца)	вручную	на однократно записываемые оптические компакт-диски	На время существования оператора

Резервирование конфигурационных файлов, программных модулей (наименование СЗИ, например, средство антивирусной защиты) не осуществляется. Для восстановления работоспособности данных СЗИ используются оптические диски с дистрибутивами СЗИ, полученные от поставщиков.

Если выполнение требования настоящей Инструкции нарушает положения лицензионного соглашения с поставщиком СЗИ, то такое требование выполнять не обязательно.

В информационной системе необходимо проводить анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных

Необходимо документировать все изменения, вносимые в базу данных системы защиты информации.

Лист согласования

Заместитель директора по учебной и инновационной работе _____ **В.А. Лихачева** 17.04.2015
Подпись Дата

Начальник информационно-вычислительного центра _____ **И.В. Картавченко** 17.04.2015
Подпись Дата

Начальник юридического отдела _____ **Е.Г.Жальских** 17.04.2015
Подпись Дата

Прошнуровано, пронумеровано
и скреплено печатью

23 (двадцать два) лист

Директор _____ О.В. Бурганова

«20» мая 2015г.