Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«УЧИЛИЩЕ ОЛИМПИЙСКОГО РЕЗЕРВА № 1»

ПРИКАЗ

08.11.2023 № 463

Санкт-Петербург

Об утверждении Политики информационной безопасности Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Училище олимпийского резерва № 1»

С целью обеспечения информационной безопасности в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении «Училище олимпийского резерва № 1»

ПРИКАЗЫВАЮ:

1. Утвердить Политику информационной безопасности Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Училище олимпийского резерва № 1» (далее — СПб ГБПОУ «УОР № 1»), согласно Приложению к настоящему приказу.
2. Отделу по обеспечению безопасности деятельности разместить настоящий приказ с Приложением на официальном сайте СПб ГБПОУ «УОР № 1».
3. Контроль за исполнением приказа оставляю за собой.

Директор **В.А. Кузнецов**

Приложение
к приказу СПб ГБПОУ «УОР № 1»
от 08.11.2023 № 463

Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«УЧИЛИЩЕ ОЛИМПИЙСКОГО РЕЗЕРВА № 1»

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ САНКТ-ПЕТЕРБУРГСКОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ «УЧИЛИЩЕ ОЛИМПИЙСКОГО РЕЗЕРВА № 1»

Санкт-Петербург
2023

СОДЕРЖАНИЕ

Термины и определения

Автоматизированная система — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Авторизация — предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ.

Аутентификация — проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Безопасность информации — защищённость информации от её нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного её тиражирования.

Бизнес-процесс — последовательность технологически связанных операций по предоставлению продуктов, услуг и/или осуществлению конкретного вида деятельности Учреждения.

Владелец актива — физическое или юридическое лицо, которое наделено административной ответственностью за руководство изготовлением, разработкой, хранением, использованием и безопасностью актива. Термин «владелец» не означает, что этот человек фактически имеет право собственности на этот актив.

Владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом.

Документ — зафиксированная на материальном носителе информация с реквизитами, позволяющими её идентифицировать.

Доступность информации — состояние, характеризуемое способностью ИС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Защита информации — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию и средства доступа к ней.

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

Информация — сведения (сообщения, данные) о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информационная безопасность (ИБ) — состояние защищённости интересов Учреждения.

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

Информационный процесс — процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

Информационный ресурс (актив) — всё, что имеет ценность и находится в распоряжении Учреждения.

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

Инцидент информационной безопасности — одно или серия нежелательных, или неожиданных событий ИБ, имеющих значительную вероятность нарушения бизнес-процессов или представляющих угрозу ИБ.

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

Конфиденциальная информация — информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность информации — состояние защищённости информации, характеризуемое способностью ИС обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.

Несанкционированный доступ — доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Обработка риска — процесс выбора и реализации мер по модификации (снижению) риска.

Политика — общие цели и указания, формально выраженные руководством.

Привилегии — это права доверенного объекта на совершение каких-либо действий по отношению к объектам системы.

Риск — сочетание вероятности события и его последствий.

Сервер — выделенный или специализированный компьютер для выполнения сервисного программного обеспечения, предназначенный для хранения информации и обеспечения доступа к ней с удалённых клиентских устройств.

Система управления информационной безопасностью (СУИБ) — часть общей системы управления, основанная на оценке рисков, предназначенная для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования ИБ.

Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, в полном объёме

реализующий полномочия владения, пользования, распоряжения указанными объектами.

События информационной безопасности — идентифицированное состояние системы, сервиса или сети, свидетельствующее о возможном нарушении политики безопасности или отсутствии механизмов защиты, либо прежде неизвестная ситуация, которая может иметь отношение к безопасности.

Угроза — опасность, предполагающая возможность потерь (ущерба).

Целостность информации — устойчивость информации к несанкционированному доступу или случайному воздействию на неё в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

Обозначения и сокращения

АРМ	—	Автоматизированное рабочее место
АС	—	Автоматизированная система
ИБ	—	Информационная безопасность
ИР	—	Информационный ресурс
ИС	—	Информационная система
КС	—	Корпоративная сеть
ИТ	—	Информационная технология
НСД	—	Несанкционированный доступ
ОКЗИ	—	Орган криптографической защиты информации
ПО	—	Программное обеспечение
СКЗИ	—	Средство криптографическое защиты информации
СУИБ	—	Система управления информационной безопасностью
ИСПДн	—	Информационная система персональных данных
ПДн	—	Персональные данные
ФСТЭК	—	Федеральная служба по техническому и экспортному контролю
ФСБ	—	Федеральная служба безопасности
ЛВС	—	Локальная вычислительная сеть
КПП	—	Контрольно-пропускной пункт
АИСУ	—	Автоматизированная информационная система управления
СКУД	—	Система контроля и управления доступом
АПС	—	Автоматическая пожарная сигнализация

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая политика информационной безопасности (далее — Политика) Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Училище олимпийского резерва № 1» (далее — Учреждения) определяет цели и задачи системы обеспечения информационной безопасности (далее — ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Учреждение в своей деятельности.

1.2. Политика разработана в рамках исполнения Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.3. Основной целью Политики является защита информации Учреждения при осуществлении уставной деятельности, которая предусматривает принятие необходимых мер в целях защиты информации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации.

1.4. Политика направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

1.5. Основными задачами Политики являются:

- разработка требований по обеспечению ИБ;
- контроль выполнения установленных требований по обеспечению ИБ;
- повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию ИБ;
- разработка нормативных документов для обеспечения ИБ Учреждения;
- выявление, оценка, прогнозирование и предотвращение реализации угроз ИБ Учреждения;
- организация антивирусной защиты информационных ресурсов Учреждения;

– защита информации Учреждения от несанкционированного доступа и утечки по техническим каналам;

– организация периодической проверки соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки директору Учреждения.

1.6. Настоящая Политика распространяется на все структурные подразделения Учреждения и обязательна для исполнения всеми его работниками и должностными лицами.

1.7. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах Учреждения, а также в договорах. Все другие политики, процедуры, мероприятия и цели, связанные с ИБ, должны быть согласованы с данной Политикой.

1.8. Актуализация настоящей политики производится по мере необходимости и имеет целью приведение в соответствие определенных политикой защитных мер реальным условиям и текущим требованиям к защите информации.

1.9. Внеплановая актуализация политики информационной безопасности производится в обязательном порядке в следующих случаях:

– при изменении политики РФ в области информационной безопасности, указов и законов РФ в области защиты информации;

– при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся информационной безопасности Учреждения;

– при происшествии и выявлении инцидента (инцидентов) по нарушению информационной безопасности, влекущего ущерб Учреждению.

2. Описание объекта информатизации

Учреждение является унитарной некоммерческой организацией, осуществляющей:

— организацию предоставления среднего профессионального образования в области физической культуры и спорта;

— организация предоставления среднего общего образования;

— обеспечением подготовки спортивных сборных команд Санкт-Петербурга по олимпийским видам спорта (далее — команды), включая обеспечение подготовки спортивного резерва для команд, в том числе осуществление спортивной подготовки;

— организацию предоставления общего образования лицам, проходящим подготовку в Учреждении и входящим в состав команд, а также лицам, проходящим подготовку в Учреждении в целях включения их в состав команд;

— организацию и проведение официальных региональных физкультурных, физкультурно-оздоровительных и спортивных мероприятий

Учреждение находится в ведении Комитета по физической культуре и спорту, осуществляющего координацию деятельности Учреждения

В информационном обмене Учреждения участвуют персональные данные: работников (сегменты сторонних ИС операторами которых Учреждение не является), обучающихся (ИСПДн АИСУ «Параграф школа», ИСПДн АИСУ «Параграф колледж», а также сегменты сторонних ИС операторами которых Учреждение не является).

Обработка персональных данных происходит в информационной системе Учреждения, которая представляет собой:

1. Сервера, расположенные в стойках в серверном помещении;
2. Коммутаторы, расположенные в серверной и распределительных шкафах, обеспечивающие взаимодействие с серверами;
3. Персональные компьютеры, находящиеся в рабочих помещениях.

Сервер ИСПДн «АИСУ «Параграф Школа» работает на виртуальной машине Hyper-V на основе семейства автоматизированных информационных систем «Параграф». ИСПДн позволяет разграничить доступ к информации для пользователей, а также функционал для сохранения целостности информации. Доступ к привилегиям администратора имеют директор Учреждения и работники, в чьих обязанностях осуществление обслуживания функционирования информационной системы. Получение данных с сервера может происходить через локальную сеть Учреждения или же, в частных случаях, через терминальное устройство, находящееся в серверном помещении.

На входе в Учреждение находится пост охраны, на котором происходит мониторинг активности камер наблюдения, СКУД, а также пожарной безопасности.

Доступ в здание Учреждения имеют работники и обучающиеся по предъявлению пропуска, который необходимо приложить к считывателю на калитке при входе на территорию и на КПП при входе. Некоторые работники, согласно должностным инструкциям, могут иметь доступ входа/выхода на территорию Учреждения и в здание Учреждения через другие входы/выходы. Для третьих лиц вход осуществляется после занесения их данных в специальный журнал или по предварительной записи. Доступ непосредственно в рабочие помещения имеют работники Учреждения и работники организаций, с которыми заключен договор об оказании каких-либо услуг, что отражается в соответствующих локальных нормативно-правовых актах. Работники Учреждения под подпись берут и сдают ключ на КПП.

Доступ в серверную происходит с помощью ключа, который хранится у лиц, которые осуществляют обеспечение работоспособности находящегося внутри оборудования.

С целью обеспечения бесперебойной подачи питания в элементах СКУД и серверного оборудования установлены накопители энергии, позволяющие некоторое время после отключения энергии обеспечивать электричеством наиболее важные элементы информационной системы.

3. Перечень организационных и технических мер защиты информации

Все меры обеспечения безопасности информационного обмена Учреждения подразделяются на следующие виды:

- нормативно-правовые;
- морально-этические;
- организационные;
- физические;
- технические.

3.1. Нормативно-правовые

К данному виду мер защиты относятся действующие законы, указы, постановления, соглашения, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных взаимодействий в процессе обработки и использовании, а также устанавливающие ответственность за нарушения этих правил. Также к данным мерам относится техническая документация применяемых СЗИ.

3.2. Морально-этические

Система морально-этических ценностей имеет особое значение в сфере осуществления образовательной деятельности. Она служит основой для содействия воплощения идей гуманизма, нравственности и социальной справедливости в профессиональной деятельности работников.

Все, что касается условий жизнедеятельности обучающихся и работников, их личностных качеств, проблем, является конфиденциальной информацией. Каждый обучающийся и работник должен быть поставлен об этом в известность.

3.3. Организационные

К данному виду мер защиты относятся меры организационного характера, регламентирующие процессы функционирования системы обработки данных (разработка внутренних локальных актов), использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности.

Главной целью организационных мер, предпринимаемых на высшем управленческом уровне – сформировать политику в области обеспечения безопасности информации и обеспечить ее выполнение, выделяя необходимые технические, финансовые и человеческие ресурсы, а также постоянно контролируя состояние дел.

3.4. Физические

Ответственность за реализацию мер защиты компьютерной сети и носителей информации физического характера несет непосредственно директор Учреждения и лица уполномоченные в части обеспечения информационной безопасности. Не допускается перекладывание этих мер на наемные охранные структуры.

К числу физических мер относятся:

– реализация пропускной системы для доступа в помещения, в которых находятся носители данных;
– создание СКУД;
– определение уровней доступа;
– наружное и внутреннее видеонаблюдение;
– создание правил обязательного регулярного резервного копирования критически важных данных.

3.5. Технические

Технические меры защиты предусматривают использование специализированного программного обеспечения, применяются рекомендованные и разрешенные антивирусы и другие виды специального программного обеспечения.

Применяемое для технической защиты программное обеспечение должно обеспечивать контроль электронной почты, которой пользуются работники Учреждения.

3.5.1. Доступ пользователей к работе с объектами информационной безопасности Учреждения и доступ к их ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей должны производиться установленным порядком, согласно регламента предоставления доступа пользователей.

3.5.2. Все работники Учреждения, зарегистрированные как легальные пользователи сети должны нести персональную ответственность за нарушения установленного порядка обработки информации, правил хранения, использования и передачи, находящихся в их распоряжении защищаемых ресурсов системы.

3.5.3. Подлежащие защите ресурсы системы подлежат строгому учету.

3.5.4. Все неиспользуемые в работе устройства ввода-вывода информации на рабочих местах работников, работающих с конфиденциальной информацией, должны быть по возможности отключены, не нужные для работы программные средства и данные с дисков также должны быть удалены.

3.5.5. В компонентах объектов информационной безопасности Учреждения и на рабочих местах пользователей должны устанавливаться и использоваться лицензионные программные средства, прошедшие антивирусную проверку.

3.5.6. Пользователи объектов информационной безопасности Учреждения должны быть ознакомлены со своими полномочиями, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации в Учреждении.

3.5.7. Любое грубое нарушение порядка и правил пользования информационными ресурсами Учреждения должно расследоваться. К виновным применяться адекватные меры воздействия.

3.5.8. Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

– индивидуальная идентификация пользователей и инициированных им процессов;

– проверка подлинности пользователей на основе паролей, ключей на различной основе и т.д.;

– реакция при попытке несанкционированного доступа (сигнализация, блокировка и т.д.);

– ведение журнала событий (регистрация всех событий).

3.5.9. Для обеспечения информационной безопасности в Учреждении необходимо использование следующих средств защиты:

– инженерно-технические;

– средства идентификации и аутентификации пользователей;

– средства разграничения доступа;

– средства обеспечения контроля и целостности;

– средства оперативного контроля и регистрации событий безопасности;

– криптографические средства;

– СКУД.

4. Регулирующие законодательные нормативные документы

Перечень регулирующих законодательных нормативных документов:

Федеральный закон «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» от 19.12.2005 № 160-ФЗ;

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требования к защите персональных данных при их обработке в информационных системах персональных данных»;

Приказ Роскомнадзора от 16.07.2010 № 482 «Об утверждении образца формы уведомления об обработке персональных данных;

Приказ Роскомнадзора от 15.03.2013 № 274 «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных»;

Приказ Роскомнадзора от 30.05.2017 № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки

персональных данных и о внесении изменений в ранее представленные сведения»;

Приказ Роскомнадзора от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения»;

ГОСТ Р ИСО/МЭК 27001 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности»;

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

Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

Методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11.02.2014;

Приказ ФСБ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

Приказ ФСБ от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

«Трудовой кодекс Российской Федерации» от 30.12.2001 № 197-ФЗ;

«Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13.06.2001 №152;

Методический документ «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 05.02.2021).

5. Политики информационной безопасности

5.1. Политика физической безопасности

Периметр зданий, в которых располагаются помещения Учреждения и его структурные подразделения, должен охраняться посредством систем видеонаблюдения с возможностью хранения информации, а также вывода информации на пульт охраны.

Все помещения Учреждения должны быть оборудованы дверьми, закрываемыми на замок. Помещения, в которых размещена ИС, используются СКЗИ в конце рабочего дня необходимо опечатывать.

Должен быть предусмотрен механизм установления личности, осуществляющей санкционированное вскрытие помещений Учреждения (например, проверка удостоверения личности, применение систем контроля и управления доступом, роспись за получение ключа от помещений на посту охраны и т.п.).

В спецпомещениях пользователей СКЗИ для хранения выданных им ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ.

Отдельные группы помещений, нахождение в которых посторонних лиц не требуется (например, архивные помещения), могут отделяться дополнительными дверьми, иными средствами ограничения доступа, опечатываться или физически располагаться удаленно (например, на других этажах или частях здания и т.п.).

Доступ в помещения Учреждения, где хранятся и обрабатываются ПДн, осуществляется согласно соответствующего Перечня работников, который утверждается директором Учреждения.

Работники Учреждения не должны оставлять свои рабочие кабинеты без наблюдения. В случае, если помещение остается без наблюдения, помещение должно быть закрыто на замок.

Работники Учреждения не должны пытаться проникнуть в помещения, доступ к которым ограничен, не имея на это соответствующих прав.

Работники сторонних организаций могут вызываться в установленном порядке, например, в случае предоставления услуг по договору, и в иных случаях, предусмотренных законодательством. При необходимости помещения работников сторонних организаций без предварительной заявки их допуск в помещения Учреждения должен осуществляться только по согласованию с ответственным лицом структурного подразделения Учреждения, в ведении которого предполагаются проводимые работы. Работники сторонних организаций должны находиться на территории Учреждения в сопровождении уполномоченных работников Учреждения.

Пункты работы с входящей и исходящей почтой и факсимильные аппараты, находящиеся без присмотра, должны быть защищены.

Использование фотокопировальных устройств и другой техники воспроизведения (например, сканеры, цифровые камеры), с целью компрометации информации, должно предотвращаться.

Документы, содержащие конфиденциальную информацию, должны удаляться с принтеров немедленно.

5.2. Политика эксплуатации электронных устройств

Размещение экранов компьютеров, обрабатывающих информацию ограниченного доступа, должно исключать возможность их просмотра лицами, не допущенными к данной информации.

При использовании систем видеонаблюдения, такие системы должны быть установлены в местах, исключающих просмотр содержимого экранов компьютеров, обрабатывающих ПДн, а также исключающих просмотр вводимых паролей, кодов и т.п.

Системные блоки должны быть опечатаны или оборудованы иным способом ограничения их несанкционированного вскрытия.

Работникам Учреждения запрещено подключать или устанавливать собственные компьютеры, периферийные устройства, в том числе съемные носители информации, комплектующие к компьютерам Учреждения на которых производится обработка ПДн.

Необходимо осуществлять периодический контроль за состоянием технических средств охраны в спецпомещениях пользователей СКЗИ.

Перед передачей (в том числе для ремонта) сторонним организациям, списанием или прекращением использования оборудования, участвующего в обработке информации ограниченного доступа, должна быть проведена проверка, с целью исключения попадания такой информации третьим лицам.

5.3. Политика обеспечения управления доступом

Работникам Учреждения запрещено осуществление противоправных действий, включая деятельность по получению несанкционированного доступа к информационным системам и ее элементам; нанесение ущерба и нарушение работы информационным системам и ее элементов; перехват паролей или иной способ получения паролей, ключевой информации или иных механизмов доступа, которые могут быть использованы для несанкционированного доступа.

Программное обеспечение, предполагающее использование механизмов разделения доступа или подразумевающее индивидуальную ответственность работника за осуществляемые действия, должно использовать механизм контроля доступа, с идентификацией и авторизацией пользователя с помощью, как минимум пароля, отвечающего требованиям политики парольной защиты.

Настройка доступа ко всем информационным ресурсам Учреждения должна быть по умолчанию направлена на предотвращение к ним любого несанкционированного доступа.

Если система контроля доступа АРМ, информационных систем вышла из строя, то по умолчанию доступ пользователей должен быть запрещен.

Доступ к информационным ресурсам Учреждения должен осуществляться согласно разработанному и утвержденному руководителем перечню, составленного на основании должностных обязанностей работников Учреждения.

Любое изменение в правах доступа к информационным ресурсам Учреждения должно быть обосновано выполнением должностных обязанностей,

утверждено и направлено лицу уполномоченному в части информационной безопасности.

При увольнении работников Учреждения или изменении их должностных обязанностей, лица, уполномоченные на предоставление прав доступа, должны быть проинформированы в трехдневный срок, после чего необходимо внести соответствующие изменения в систему контроля доступа и перечни доступа.

Для установления персональной ответственности идентификатор учетной записи пользователя в любой информационной системе должен однозначно соответствовать отдельному работнику.

Компьютеры и терминалы должны быть оставлены в состоянии выполненного выхода из системы или подобным механизмом аутентификации пользователя, когда они находятся без присмотра, и должны быть защищены паролями или другими средствами управления, когда не используются.

Для доступа к АРМ и информационным системам Учреждения у каждого пользователя должны быть уникальный набор из идентификатора учетной записи и пароля. Запрещено создание идентификатора учетной записи, используемого группой лиц.

Использование идентификатора учетной записи пользователя после увольнения или прекращения использования информационных ресурсов Учреждения запрещено.

При предоставлении идентификатора учетной записи сторонним организациям необходимо заключение соглашений, подтверждающих обязательства сторонних организаций соблюдать требования НПА РФ и организационно-распорядительных документов Учреждения, подписанные уполномоченными лицами.

При прекращении необходимости использования сторонними организациям идентификатора учетной записи, лица, уполномоченные на предоставление прав доступа, должны быть письменно проинформированы в однодневный срок, после чего должны быть внесены соответствующие изменения в систему контроля доступа.

Для всех лиц, не являющихся работниками Учреждения, но для выполнения обязательств которых необходимо предоставление доступа к АРМ и информационным системам Учреждения, должен быть сформирован идентификатор учетной записи, действующий только на период выполнения лицом своих обязательств. В случае, если срок выполнения обязательств не определен, то срок действия идентификатора учетной записи должен составлять 60 дней.

Пользователям запрещено использование идентификаторов учетных записей и паролей, используемых для получения доступа к информационным ресурсам Учреждения, для идентификации и аутентификации на публичных ресурсах сетей общего пользования.

Все информационные системы и технические средства должны поддерживать специальный тип учетной записи, позволяющий производить

любые поддерживаемые настройки и изменения, включая изменения в системе обеспечения безопасности.

Количество таких типов учетных записей должно быть максимально ограничено и предоставлено только тем пользователям, которым это необходимо для осуществления должностных обязанностей с учетом соблюдения требований НПА РФ и организационно-распорядительных документов Учреждения.

Пользователям запрещено собирать и копировать информацию с информационных ресурсов, если это не обусловлено выполнением должностных обязанностей. При наличии технической возможности используемые системы контроля доступа должны предупреждать возможность таких действий и информировать о таких попытках.

5.4. Политика обеспечения сетевой безопасности

Конфигурация и настройка всех устройств, подключенных к корпоративной сети Учреждения должны соответствовать требованиям НПА РФ и организационно-распорядительным документам Учреждения.

Размещение в информационных системах Учреждения информации ограниченного доступа должно соответствовать требованиям НПА РФ и организационно-распорядительным документам Учреждения.

Используемые внешние интерфейсы и протоколы корпоративной сети Учреждения должны быть максимально ограничены необходимыми для обеспечения выполнения Учреждением своих задач и функций.

Технические средства, обеспечивающие работу корпоративной сети, должны размещаться с соблюдением требований по контролю физического доступа к ним и организации их сохранности.

Для управления техническими устройствами в сети по возможности должны быть использованы протоколы, поддерживающие криптографическую защиту информации.

5.5. Построение локальной вычислительной сети Учреждения

Все локальные сети Учреждения должны быть настроены для недопущения несанкционированного подключения к ним и обнаружения попыток таких подключений.

Подключение к локальной вычислительной сети Учреждения разрешено только после выполнения требований политик безопасности и критериев, определенных Учреждением.

Настройка маршрутизаторов должна осуществляться в соответствии с рекомендациями производителя, обеспечивающими максимальный уровень безопасности.

Доступ к программным настройкам активных технических средств корпоративной сети должен быть ограничен паролем, отвечающим требованиям политики парольной защиты Учреждения.

5.6. Политика использования программного обеспечения

Программное обеспечение, используемое для осуществления деятельности структурных подразделений Учреждения, должно соответствовать условиям его лицензирования (независимо от того, является ли оно коммерческим или свободно распространяемым) и использоваться строго в соответствии с лицензионным соглашением. Любое структурное подразделение Учреждения должно исключить случаи хранения и/или использования программного обеспечения, не являющегося лицензионным.

В случае если в НПА РФ предъявляются особые требования к программному обеспечению (например, требование по сертификации такого программного обеспечения уполномоченными организациям и т.п.) Учреждение обязан обеспечить хранение документов, подтверждающих прохождения данного программного обеспечения сертификации и т.п.

На каждый рабочий компьютер должен быть установлен комплект программного обеспечения, необходимый и достаточный для выполнения на нем поставленных задач.

Учреждение предоставляет работникам достаточное количество лицензий на использование программного обеспечения, необходимого для выполнения должностных обязанностей.

Обновление версий программного обеспечения, использующего ресурсы КС, должно осуществляться только администраторами информационных систем или уполномоченными лицами. Допустимо использование функции автоматического обновления программного обеспечения, использующего ресурсы сети Учреждения.

Пользователям запрещено выполнение команд уровня операционной системы или предпринимать попытки их выполнения. Действия пользователя должны быть ограничены взаимодействием с элементами экранных форм программного обеспечения, необходимым для выполнения должностных обязанностей.

При увольнении или изменении должностных обязанностей пользователя, файлы, содержащиеся на его АРМ, должны быть проверены его непосредственным руководителем, или уполномоченным лицом, и, в случае необходимости, переданы другим исполнителям.

5.7. Политика парольной защиты

Доступ к АРМ, используемому пользователями в рамках должностных обязанностей и подразумевающему наличие идентификации и аутентификации пользователя и/или разграничение полномочий без использования пароля запрещено.

Пароли доступа к различному прикладному программному обеспечению, используемому пользователями и администраторами в рамках должностных обязанностей должны отличаться от паролей доступа к АРМ или элементам сетевой инфраструктуры и не должны совпадать для различного программного обеспечения.

В нормативно-правовой базе должен быть документ, определяющий Политику Учреждения в части работы с паролями, регламентирующий действия по назначению, смене, хранению паролей, действия при компрометации, восстановлении утерянных паролей.

5.8. Политика антивирусной защиты

Антивирусное программное обеспечение должно быть установлено и функционировать в штатном режиме на всех компьютерах, выполняющих функции серверов корпоративной сети Учреждения, на всех АРМ отдельно стоящих и подключенных к корпоративной сети и на всех портативных компьютерах.

Не допускается изменение настроек системы антивирусной защиты, в части оповещения о нахождении компьютерных вирусов или вредоносных программ, в результате действия которых уменьшается эффективность работы информационных систем.

Обновления баз системы антивирусной защиты должно производиться регулярно. Построение системы антивирусной защиты должно предусматривать возможность обновления ее антивирусных баз и компонентов производителем по мере их создания. В случае невозможности такого построения системы (например, отдельно стоящие АРМ не подключенные к каким-либо сетям), обновление системы антивирусной защиты должно производиться с регулярностью, обеспечивающей ее эффективное функционирование.

Запрещается отключение системы антивирусной защиты, за исключением случаев проведения тестирования программного обеспечения и иных тестов, проводимых уполномоченными работниками Учреждения.

Структурные подразделения Учреждения обязаны проводить сканирование своих информационных ресурсов, а также всех подключенных АРМ на наличие компьютерных вирусов и/или вредоносных программ.

Файлы, полученные любым образом, с любых носителей информации или сетей общего пользования должны быть проверены на наличие вредоносного кода.

Подключения к АРМ незарегистрированных отчуждаемых носителей информации (дискеты, компакт-диски, съемные жесткие диски, сотовые телефоны, карманные персональные компьютеры, фотоаппараты и иные носители информации) разрешено с обязательной проверкой «по требованию» таких носителей информации на наличие компьютерных вирусов и/или вредоносных программ.

В случае получения файлов, проверка которых в исходном состоянии невозможна (например, файлы содержат архивы, не поддерживаемые системой антивирусной защиты, файлы прошли криптографическое преобразование и т.п.), необходимо на АРМ, не подключенном к корпоративной сети Учреждения, привести данные файлы к состоянию пригодному для проверки на наличие вредоносного кода, осуществить такую проверку, после чего принимать решение о возможности использования данных файлов.

Все файлы, передаваемые третьим лицам, должны быть проверены на наличие вредоносного кода системой антивирусной защиты до их передачи.

Любые намеренные попытки написания, компиляции, хранения, запуска, пропагандирования или распространения пользователями компьютерных вирусов или вредоносных программ, а также иного кода, предназначенного для саморазмножения, нанесения ущерба или снижения производительности информационных систем Учреждения, запрещены.

В случае обнаружения системой антивирусной защиты компьютерного вируса или вредоносной программы пользователь обязан прекратить работу и сообщить об этом администратору информационной безопасности или иному уполномоченному лицу в части информационной безопасности.

О любом инциденте, связанном с выявлением компьютерного вируса или вредоносных программ, на АРМ или портативном компьютере, подключаемом к сети Учреждения, должно быть сообщено администратору информационной безопасности.

Самостоятельные попытки пользователя по удалению компьютерного вируса или вредоносной программы запрещены.

5.9. Политика использования сети Интернет

Вся информация, полученная из сети Интернет, должна считаться недостоверной, не будучи подтвержденной из других источников. Перед использованием свободно распространяемой информации из сети Интернет для принятия решений в рамках деятельности Учреждения, такая информация должна быть перепроверена в других источниках.

Учреждение не несет ответственности за информацию, содержащуюся в сети Интернет. В случае открытия пользователем ресурсов, содержание которых может считаться незаконным или оскорбительным пользователь обязан прекратить работу с данным ресурсом.

Для получения возможности доступа пользователя в сети Интернет должны быть обеспечены механизмы защиты информационных ресурсов Учреждения от воздействия из сети Интернет (межсетевой экран).

Передача информации ограниченного доступа по сетям общего пользования, допускается при условии соблюдения всех требований к такой передаче. Передача информации ограниченного доступа без соблюдения требований, предъявляемых к ее передаче по сети Интернет, запрещена.

Пользователю запрещено любое тестирование и/или попытки обхода установленных механизмов защиты информационных ресурсов Учреждения.

Запрещено предоставлять доступ к сети Интернет стороннему обслуживающему персоналу, консультантам и иным лицам, состоящим в договорных отношениях с Учреждением, за исключением случаев, когда такой доступ необходим для решения данными лицами задач в интересах структурных подразделений Учреждения. Доступ может быть предоставлен только по согласованию с уполномоченным лицом структурного подразделения Учреждения, а в случае использования корпоративной сети Учреждения –

с администратором информационной безопасности или с иным уполномоченным лицом в части информационной безопасности.

Использование сети Интернет для личных нужд пользователя запрещен. Доступ пользователям предоставляется к сети Интернет для выполнения должностных обязанностей. Пользователям запрещена загрузка любого программного обеспечения из сети Интернет. В исключительных случаях, когда загрузка такого программного обеспечения продиктована соблюдением интересов Учреждения, загрузка программного обеспечения из сети Интернет осуществляется уполномоченными лицами структурных подразделений Учреждения.

Работникам Учреждения запрещено участвовать в обмене пиратским программным обеспечением, серийными номерами программного обеспечения и ином обмене, нарушающем и/или ущемляющем права правообладателей обмениваемой информации.

При наличии технической возможности, Учреждение может обеспечить работникам беспроводной канал (например, Wi-Fi) доступа в сеть Интернет для выполнения должностных обязанностей, в части поиска, сбора, анализа информации, однако доступ во внутреннюю сеть и информационные системы Учреждения через беспроводной канал должен быть запрещен.

5.10. Политика использования электронной почты

Электронная почта должна быть использована работниками Учреждения только для выполнения должностных обязанностей, выполнения договорных обязательств Учреждения и выполнения требований НПА РФ.

Запрещено использовать электронную почту для отправления писем следующего содержания:

– писем, содержащих конфиденциальную информацию, в том числе персональные данные, обрабатываемые и охраняемые в Учреждении;

– писем, содержание которых может считаться незаконным или оскорбительным, например, материалы сексуального характера, расистские, дискредитирующие, оскорбительные, непристойные, уничижительные, дискриминационные, угрожающие, или иные подобные сообщения;

– любых подрывных, оскорбительных, неэтичных, незаконных или недопустимых материалов, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возрасте, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений или о национальном происхождении, гиперссылок или других ссылок на неприличные или очевидно оскорбительные веб-сайты и подобные материалы, шутки, массовые рассылки, предупреждений о вирусах и розыгрышей, обращений о помощи или вредоносного кода;

– писем, написанных таким образом, который может быть интерпретирован как официальная позиция или высказывание Учреждения, если это не разрешено руководителем Учреждения в соответствии с нормативно-методическими документами Учреждения.

Запрещено использовать электронную почту в следующих целях:

- отправки сообщения с чужого почтового ящика или от чужого имени;
- отправки сообщений в личных или благотворительных целях, не связанных с деятельностью Учреждения;
- массовой рассылки писем, кроме случаев, когда необходимо оповещение большого числа работников Учреждения или в случаях, когда это обусловлено выполнением задач Учреждения;
- в любых других незаконных, неэтичных и неразрешенных целях.

Работники Учреждения, получившие электронную почту от другого пользователя Учреждения, с сообщениями, содержащими запрещенное содержание обязаны уведомить о таком факте администратора информационной безопасности или иному уполномоченному лицу в части информационной безопасности.

Использование электронной почты должно осуществляться с применением технологий идентификации и аутентификации пользователя. Также, рекомендуется использование двухфакторной аутентификации.

Отправка электронной почты, содержащей информацию ограниченного доступа, должна осуществляться в соответствии с требованиями, предъявляемыми к такой информации.

Пользователям запрещено открывать вложения в электронные сообщения, в случае если отправитель данного сообщения не известен пользователю.

Пользователям запрещено отвечать на запросы любой персональной идентификационной информации, включая пароли, коды доступа, номера кредитных карт и т.п. В случае получения сообщений с такими запросами пользователь обязан сообщить о них администратору информационной безопасности или иному уполномоченному лицу в части информационной безопасности.

5.11. Политика использования отчуждаемых носителей

Использование личных отчуждаемых носителей информации запрещено для всех работников Учреждения.

Работники, которым необходимо использование отчуждаемых носителей информации для выполнения должностных обязанностей, должны быть обеспечены такими носителями.

Служебные отчуждаемые носители информации должны подлежать учету, а их передача работникам должна быть подтверждена их росписью. Работник несет персональную ответственность за их сохранность. Работникам запрещено создавать предпосылки для осуществления утраты, кражи и иных противоправных действий со служебными отчуждаемыми носителями информации.

Использование отчуждаемых носителей информации для хранения информации ограниченного доступа должно соответствовать требованиям НПА РФ и внутренних документов Учреждения.

Использование служебных отчуждаемых носителей информации в личных целях запрещено.

Подключение служебных отчуждаемых носителей информации к техническим средствам, заведомо содержащим вирусы и/или вредоносные программы, запрещено. В этом случае отчуждаемые носители передаются администратору информационной безопасности или иному уполномоченному лицу в части информационной безопасности.

Эксплуатация отчуждаемых носителей информации должна осуществляться в соответствии с требованиями по их эксплуатации, и направлена на предупреждение их неисправности.

5.12. Политика использования средств криптографической защиты

Деятельность со средствами криптографической защиты должна исключать нарушение законодательства Российской Федерации в области лицензирования. В случае, если предполагаемая деятельность со средствами криптографической защиты подразумевает необходимость получения лицензии, то учреждение обязано получить такую лицензию или привлекать для подобной деятельности сторонние организации, имеющие соответствующие лицензии.

При использовании средств криптографической защиты для защиты информации ограниченного доступа данные криптографические средства должны соответствовать требованиям НПА РФ.

Установка, настройка и техническое сопровождение средств криптографической защиты должно осуществляться квалифицированными специалистами и не нарушать требования НПА РФ.

Использование, в том числе хранение, средств криптографической защиты должно отвечать требованиям законодательства Российской Федерации.

Перед использованием средств криптографической защиты работники обязаны пройти обучение по порядку их использования.

Пользователям запрещено использование средств криптографической защиты других пользователей, в том числе с целью выдать себя за другого пользователя.

Все действия по обеспечению сохранности ключей должны быть направлены на исключение компрометации ключей.

В случае компрометации ключей или подозрения на компрометацию пользователь обязан прекратить любое использование средств криптографической защиты и незамедлительно сообщить о данном факте уполномоченному лицу Учреждения.

5.13. Политика резервного копирования

Резервное копирование информации, размещенной на АРМ пользователей и компьютерах, выполняющих функции сервера КС, осуществляется уполномоченным лицом Учреждения.

Политика резервного копирования распространяется только на рабочую информацию, хранящуюся на информационных ресурсах Учреждения.

Регулярность создания резервных копий рабочей информации должна быть достаточной для продолжения нормальной работы Учреждения, в случае нарушения целостности и/или доступности рабочей информации на информационных ресурсах Учреждения.

Все резервные копии, должны быть размещены в отдельных каталогах, название которых отражает дату последнего изменения рабочей информации и ее краткое описание.

Вся рабочая информация, хранящаяся на аппаратных ресурсах Учреждения и копируемая на отчуждаемые носители, должна быть доступна для дальнейшего восстановления.

Порядок хранения резервных копий информации ограниченного доступа определяется отдельными требованиями по защите информации ограниченного доступа.

Срок хранения резервных копий на внешних носителях определяется регламентом резервного копирования, если иное не определено НПА РФ, или организационно-распорядительными документами Учреждения.

Резервные копии, хранящиеся более полугода, должны ежеквартально тестироваться, для подтверждения возможности их восстановления и использования.

5.14. Кадровая политика

Претендентам на работу не должна раскрываться информация об имеющейся системе защиты информации.

До начала выполнения своих должностных обязанностей до претендента должна быть доведена вся необходимая информация и проведены все инструктажи в соответствии с требованиями НПА РФ и организационно-распорядительной документации Учреждения.

Ответственное выполнение требований по информационной безопасности является обязанностью всех работников Учреждения. Требования по информационной безопасности касаются всех работников Учреждения.

Для выполнения требований по информационной безопасности работники должны знать требования НПА РФ и организационно-распорядительной документации Учреждения, регламентирующие данные требования и письменно подтверждать свое согласие на их выполнение.

Невыполнение требований НПА РФ и организационно-распорядительной документации Учреждения по защите информации является поводом для проведения служебных расследований и возможному привлечению к дисциплинарной, административной и уголовной ответственности в соответствии с действующим законодательством Российской Федерации и административно-правовыми нормами, установленными в Учреждении.

Для выполнения требований по информационной безопасности пользователям запрещено прибегать к помощи третьих лиц, без согласования с руководителем Учреждения.

При увольнении или прекращении договорных обязательств работники должны быть уведомлены и согласны с требованиями по неразглашению информации ограниченного доступа и сведений о системе защиты информации в Учреждении, в соответствии с НПА РФ и организационно-распорядительной документацией Учреждения.

- система защиты персональных данных
- система защиты персональных данных (СЗПДн), строится на основании:
- перечня персональных данных, подлежащих защите;
- акта классификации информационной системы персональных данных;
- модели угроз безопасности персональных данных;
- руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Учреждения. На основании анализа актуальных угроз безопасности ПДн, описанного в Модели угроз, и Акта о результатах проведения проверки делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а также программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей;
- сервера приложений;
- СУБД;
- граница ЛВС;
- каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, система защиты ПДн может включать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевого экранирования;
- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечение целостности данных;
- обнаружение вторжений.

6. Распределение ролей и ответственности субъектов

Руководство Учреждения обязуется выполнять требования по ИБ, а также поддерживать постоянное совершенствование всех видов деятельности.

Все работники Учреждения, зарегистрированные как легальные пользователи информационной системы и обслуживающий персонал, должны нести персональную ответственность за нарушения установленного порядка обработки информации, правил хранения, использования и передачи, находящихся в их распоряжении защищаемых ресурсов системы. Каждый работник должен подписывать обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению конфиденциальной информации, а также правил работы с информацией.

Предполагается возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

Любое грубое нарушение порядка и правил пользования информационными ресурсами должно расследоваться. К виновным должны применяться адекватные меры воздействия. Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной работы с информацией, должна определяться нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению руководства.

Для создания необходимой юридической основы процедур привлечения работников к ответственности за нарушения в области информационной безопасности необходимо, чтобы:

- во всех положениях о структурных подразделениях и в функциональных (технологических) обязанностях всех работников, участвующих в процессах автоматизированной обработки информации, были отражены требования по обеспечению информационной безопасности при работе в информационных системах и при обработке конфиденциальной информации;
- каждый работник (при приеме на работу) подписывал Соглашение-обязательство о соблюдении установленных требований по работе с конфиденциальной информацией;
- все пользователи были ознакомлены с перечнем сведений, подлежащих защите, в части их касающейся (в соответствии со своим уровнем полномочий);
- доведение требовании, организационно-распорядительных документов по вопросам информационной безопасности до лиц, допущенных к обработке защищаемой информации, осуществлялось руководителями подразделений под роспись.

Работники Учреждения несут ответственность по действующему законодательству за разглашение сведений конфиденциального характера,

и сведений ограниченного распространения, ставших им известными по роду работы.

Любое грубое нарушение порядка и правил работы работниками структурных подразделении должно расследоваться. К виновным должны применяться адекватные меры воздействия.

Нарушения установленных правил и требований по ИБ являются основанием для применения к работнику (исполнителю) административных мер наказания, вплоть до увольнения и привлечения к уголовной или дисциплинарной ответственности.

Мера ответственности работников за действия, совершенные в нарушение установленных правил обеспечения безопасности информации, должна определяться с учетом нанесенного ущерба, наличия злого умысла и других факторов по усмотрению руководства.

Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

– индивидуальная идентификация пользователей и инициированных ими процессов, т.е. установление за ними идентификатора (login, Username), на базе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности доступа;

– проверка подлинности пользователей (аутентификация) на основе паролей, ключей на различной физической основе, биометрических характеристик личности и т.п.;

– реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).