Краевое государственное бюджетное профессиональное образовательное учреждение
«Барнаульский государственный педагогический колледж»
(КГБПОУ «БГПК»)

Самолетов Михаил Борисович

Подписано цифровой подписью: Самолетов Михаил Борисович
Дата: 2021.06.04 19:11:44 +07'00'

Приложение №1
к Приказу № 205
от «05»сентября 2016 г

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КГБПОУ «Барнаульский государственный педагогический колледж»

Содержание

Термины и определения

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

Администратор информационной безопасности – специалист или группа специалистов Общества, осуществляющих контроль за обеспечением защиты информации в ЛВС, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Анализ риска – систематическое использование информации для определения источников и оценки риска.

Аудит информационной безопасности – процесс проверки выполнения установленных требований по обеспечению информационной безопасности. Может проводиться как самим Учреждением (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит). Результаты проверки документально оформляются свидетельством аудита.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Чаще всего аутентификация выполняется путем набора пользователем своего пароля на клавиатуре компьютера.

Доступ к информации – возможность получения информации и ее использования.

Жизненный цикл – непрерывный процесс, который начинается с момента принятия решения о необходимости создания системы и заканчивается в момент ее полного изъятия из эксплуатации.

Защищенный канал передачи данных – логические и физические каналы сетевого взаимодействия, защищенные от прослушивания потенциальными злоумышленниками средствами шифрования данных (средствами VPN), либо путем их физической изоляции и размещения на охраняемой территории.

Идентификатор доступа – уникальный признак субъекта или объекта доступа.

Идентификация – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация – это актив, который, подобно другим активам Учреждения, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Информационная безопасность – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности

информационных активов общества в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов Учреждения.

Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач подразделений Учреждения. В Учреждении используются различные типы информационных систем для решения управленческих, учетных, обучающих и других задач.

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

Информационные активы – информационные системы, информационные средства, информационные ресурсы.

Информационные средства – программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

Информационные ресурсы – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.

Инцидент информационной безопасности – действительное, предпринимаемое или вероятное нарушение информационной безопасности, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов Учреждения.

Источник угрозы – намерение или метод, нацеленный на умышленное использование уязвимости, либо ситуация или метод, которые могут случайно проявить уязвимость.

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

Конфиденциальность – доступ к информации только авторизованных пользователей.

Критичная информация – информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование подразделений Учреждения или иного вида ущерба.

Локальная вычислительная сеть – группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

Межсетевой экран – программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав сети, а также между сетью Учреждения и внешними сетями (сетью Интернет).

Мониторинг информационной безопасности – постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности, сбор, анализ и обобщение результатов наблюдения под заданные цели. Объектом мониторинга в зависимости от целей может быть автоматизированная система или ее часть, информационные технологические процессы Учреждения, информационные услуги Учреждения и пр.

Несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Обработка риска – процесс выбора и осуществления мер по модификации риска.

Остаточный риск – риск, остающийся после обработки риска.

Политика информационной безопасности – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в Учреждении для обеспечения его информационной безопасности.

Пользователь локальной вычислительной сети – сотрудник Учреждения (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в сети в установленном порядке и получивший права на доступ к ресурсам сети в соответствии со своими функциональными обязанностями.

Принятие риска – решение принять риск.

Программное обеспечение – совокупность прикладных программ, установленных на сервере или ЭВМ.

Рабочая станция – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

Регистрационная (учетная) запись пользователя – включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название подразделения, телефоны, E-mail и т.п.

Роль – совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.

Система менеджмента информационной безопасности (СМИБ) – та часть общей системы менеджмента, которая основана на подходе бизнес-рисков при создании, внедрении, функционировании, мониторинге, анализе, поддержке и совершенствовании информационной безопасности.

Система управления информационной безопасностью (СУИБ) – часть общей системы управления организации, основанная на оценке бизнес рисков, которая создает, реализует, эксплуатирует, осуществляет мониторинг, пересмотр, сопровождение и совершенствование информационной безопасности. Включает в себя организационную структуру, политики, планирование, должностные обязанности, практики, процедуры, процессы и ресурсы.

Ответственный за техническое обеспечение – сотрудник Учреждения, занимающийся сопровождением автоматизированных систем, отвечающий за функционирование локальной сети Учреждения и ПК.

Список контроля доступа – правила фильтрации сетевых пакетов, настраиваемые на маршрутизаторах и МЭ, определяющие критерии фильтрации и действия, производимые над пакетами.

Собственник – лицо или организация, которые имеют утвержденные обязательства по менеджменту для контроля разработки, поддержки, использования и безопасности активов. Термин «собственник» не означает, что лицо действительно имеет какие-либо права собственности на актив.

Средства криптографической защиты информации – средства шифрования, средства имитозащиты, средства электронной подписи, средства кодирования, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

Угрозы информационным данным – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т.е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

Управление информационной безопасностью – совокупность целенаправленных действий, осуществляемых в рамках политики информационной безопасности в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер).

Уязвимость – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности Учреждения при реализации угроз в информационной сфере.

Целостность информации – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца ключа подписи, а также установить отсутствие искажения информации в электронном документе.

VPN (VIRTUAL PRIVATE NETWORK) – «Виртуальная частная сеть»: технология и организация систематической удаленной связи между выбранными группами узлов в крупных распределенных сетях.

1. Обозначения и сокращения

АИБ – Администратор информационной безопасности.
АРМ – Автоматизированное рабочее место.
АС – Автоматизированная система.
БД – База данных.
ЗИ – Защита информации.
ИБ – Информационная безопасность.
ИР – Информационные ресурсы.
ИС – Информационная система.
ИТС – Информационно-телекоммуникационная система.
КЗ – Контролируемая зона.

МЭ – Межсетевой экран.
НСД – Несанкционированный доступ.
ОС – Операционная система.
ПБ – Политики безопасности.
ПДн – Персональные данные.
ПО – Программное обеспечение.
СВТ – Средства вычислительной техники.
СЗИ – Средство защиты информации.
СКЗИ – Средство криптографической защиты информации.
СПД – Система передачи данных.
СУБД – Система управления базами данных.
СУИБ – Система управления информационной безопасностью.
СЭД – Система электронного документооборота.
ЭВМ – Электронная - вычислительная машина, персональный компьютер.
ЭЦП – Электронная цифровая подпись.
ACL – Список контроля доступа.

1.1. Вводные положения

1.2. Введение

Политика ИБ КГБПОУ «Барнаульский государственный педагогический колледж» (далее – Учреждение) определяет цели и задачи системы обеспечения ИБ и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Учреждение в своей деятельности.

1.3. Цели

Основными целями политики ИБ являются защита информации Учреждения **от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи** и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в его Уставе.

Общее руководство обеспечением ИБ осуществляется ответственным по вопросам информационных технологий. Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет АИБ. Ответственность за функционирование автоматизированной системы Учреждения несет системный администратор.

Должностные обязанности АИБа и системного администратора закрепляются в соответствующих инструкциях.

Руководители структурных подразделений Учреждения ответственны за обеспечение выполнения требований ИБ в своих подразделениях.

Сотрудники Учреждения обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других документов ИБ.

1.4. Задачи

Политика ИБ 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.

Наибольшими возможностями для нанесения ущерба Учреждению обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне Учреждения), либо иметь непреднамеренный ошибочный характер. Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией персонала и его способностью к адекватным действиям в нештатной ситуации.

Для противодействия угрозам ИБ в Учреждении на основе имеющегося опыта составляется прогностическая модель предполагаемых угроз и модель нарушителя. Чем точнее сделан прогноз (составлены модель угроз и модель нарушителя), тем ниже риски нарушения ИБ при минимальных ресурсных затратах.

Разработанная на основе прогноза политика ИБ и в соответствии с ней построенная СУИБ является наиболее правильным и эффективным способом добиться минимизации рисков нарушения ИБ для Учреждения. Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

Стратегия обеспечения ИБ заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала.

Задачами настоящей политики являются:

- описание организации СУИБ в Учреждении;
- определение Политик ИБ, а именно:
  - Политика реализации антивирусной защиты;
  - Политика учетных записей;
  - Политика предоставления доступа к ИР;
  - Политика использования паролей;
  - Политика защиты АРМ;
  - Политика конфиденциального делопроизводства;
- определение порядка сопровождения ИС Учреждения.

1.5. Область действия

Настоящая Политика распространяется на все структурные подразделения Учреждения и обязательна для исполнения всеми его сотрудниками и должностными лицами. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

1.6. Период действия и порядок внесения изменений

Настоящая Политика вводится в действие приказом руководителя Учреждения.

Политика признается утратившей силу на основании приказа руководителя Учреждения.

Изменения в политику вносятся приказом руководителя Учреждения.

Инициаторами внесения изменений в политику информационной безопасности являются:

- Директор.
- Ответственный по вопросам информационных технологий.
- Специалист по кадрам.
- Администратор информационной безопасности.
- Системный администратор.

Плановая актуализация настоящей политики производится ежегодно и имеет целью приведение в соответствие определенных политикой защитных мер реальным условиям и текущим требованиям к защите информации.

Внеплановая актуализация политики ИБ и производится в обязательном порядке в следующих случаях:

- при изменении политики РФ в области ИБ, указов и законов РФ в области защиты информации;
- при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся ИБ Учреждения;
- при происшествии и выявлении инцидента (инцидентов) по нарушению ИБ, влекущего ущерб Учреждению.

Ответственными за актуализацию политики ИБ (плановую и внеплановую) несет АИБ.

Контроль за исполнением требований настоящей политики и поддержанием ее в актуальном состоянии возлагается на АИБа.

2. **Политики** информационной безопасности **Учреждения**

2.1. Назначение политик информационной безопасности

Политики ИБ Учреждения – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в Учреждении.

Политики ИБ относятся к административным мерам обеспечения ИБ и определяют стратегию Учреждения в области ИБ.

Политики ИБ регламентируют эффективную работу СЗИ. Они охватывают все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях. Политики ИБ реализуются посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Все документально оформленные решения, формирующие Политики, должны быть утверждены руководителем Учреждения.

2.2. Основные принципы обеспечения информационной безопасности

Основными принципами обеспечения ИБ являются следующие:

– постоянный и всесторонний анализ информационного пространства Учреждения с целью выявления уязвимостей информационных активов;

– своевременное обнаружение проблем, потенциально способных повлиять на ИБ Учреждения, корректировка моделей угроз и нарушителя;

– разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей Учреждения, а также повышать трудоемкость технологических процессов обработки информации;

– контроль эффективности принимаемых защитных мер;

– персонификация и адекватное разделение ролей и ответственности между сотрудниками Учреждения, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

2.3. Соответствие Политики безопасности действующему законодательству

Правовую основу политик составляют законы РФ и другие законодательные акты, определяющие права и ответственность граждан, сотрудников и государства в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.

2.4. Ответственность за реализацию политик информационной безопасности

Ответственность за разработку мер и контроль обеспечения защиты информации несёт АИБ.

Ответственность за реализацию политик возлагается:

– в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты – на АИБа;

– в части, касающейся доведения правил политик до сотрудников Учреждения, а также иных лиц (см. область действия настоящей политики) – на АИБа;

– в части, касающейся исполнения правил политики, – на каждого сотрудника Учреждения, согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей политики.

2.5. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе

Организация просвещения сотрудников Учреждения в области ИБ возлагается на АИБа. Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по информационной безопасности». Обучение сотрудников Учреждения правилам обращения с КИ, проводится путем:

– проведения АИБом инструктивных занятий с сотрудниками, принимаемыми на работу в Учреждении;

– самостоятельного изучения сотрудниками внутренних нормативных документов Учреждения.

Допуск персонала к работе с защищаемыми ИР Учреждения осуществляется только после его ознакомления с настоящими политиками, а также после ознакомления пользователей с «Инструкцией по работе пользователей в АС» Учреждения, а так же иными инструкциями пользователей отдельных ИС. Согласие на соблюдение правил и требований настоящих политик подтверждается подписями сотрудников в «Журнале проведения инструктажа по информационной безопасности».

Допуск персонала к работе с КИ Учреждения осуществляется после ознакомления с «Инструкцией по организации работы с материальными носителями персональных данных», «Инструкцией по организации работы с электронными носителями персональных данных и другой конфиденциальной информации». Правила допуска к работе с ИР лиц, не являющихся сотрудниками Учреждения, определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

2.6. Защищаемые информационные ресурсы Учреждения

Различаются следующие категории ИР, подлежащих защите в Учреждении.

Конфиденциальная – информация, определенная в соответствии с Федеральным Законом от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», ФЗ от 27.07.2006 г. №152-ФЗ «О персональных данных», указом президента РФ от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера», постановлением правительства РФ от 1 ноября 2012 г. №1119 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», предусмотренная «Перечнем сведений конфиденциального характера».

Публичная – информация, получаемая из публичных источников (публикации в СМИ, теле и радиовещание и т.д.). Информация, предназначенная для размещения на внешних публичных ресурсах;

Открытая – информация, полученная от физических или юридических лиц, запрет на распространение и обработку которой был ими официально снят. Информация, сформированная в результате деятельности Учреждения, которую запрещено относить конфиденциальной на основании законодательства России. Информация, представляемая в публичный доступ, используемая в хозяйственной деятельности Учреждения

Ограниченного доступа – информация, не попадающая под остальные категории, доступ к которой должен быть ограничен определенной категории лиц.

КИ представляет собой сведения ограниченного доступа, включая ПДн, для которых в качестве основной угрозы безопасности рассматривается нарушение конфиденциальности путем раскрытия ее содержимого третьим лицам, не допущенным в установленном порядке к работе с этой информацией.

Правила отнесения информации к конфиденциальной и порядок работы с конфиденциальными документами, определяются «Инструкцией по работе с конфиденциальной информацией», а также «Перечнем сведений конфиденциального характера».

Подходы к решению проблемы защиты информации в Учреждении в общем виде, сводятся к исключению неправомерных или неосторожных действий со сведениями, относящимися к информации ограниченного распространения, а также с ИР, являющимися критичными для обеспечения функционирования процессов Учреждения.

Для этого в Учреждении выполняются следующие мероприятия:

– определяется порядок работы с документами, образцами изделий и др., содержащими конфиденциальные сведения;

– устанавливается круг лиц и порядок доступа к подобной информации;

– вырабатываются меры по контролю обращения с документами, содержащими конфиденциальные сведения;

– включаются в трудовые договоры с сотрудниками обязательства о неразглашении конфиденциальных сведений и определяются санкции за нарушения порядка работы с ними и их разглашение.

При приеме на работу в Учреждение всеми сотрудниками одновременно с заключением трудового договора подписывается «Обязательство о неразглашении сведений конфиденциального характера». Защита КИ, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых Учреждением с другими организациями.

Кроме того, в Учреждении осуществляется защита ПДн сотрудников. Под персональными данными сотрудника понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника.

Согласно Ст.86 п.7 Трудового кодекса РФ защита ПДн сотрудника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

Согласно Ст.88 Трудового кодекса РФ при передаче ПДн сотрудника работодатель должен соблюдать следующие требования:

– осуществлять передачу ПДн сотрудника в пределах одной организации в соответствии с локальным нормативным актом организации, с которым сотрудник должен быть ознакомлен под расписку;

– разрешать доступ к ПДн сотрудников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные сотрудника, которые необходимы для выполнения конкретных функций.

Согласно Ст.90 Трудового кодекса РФ лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн сотрудника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

2.7. Организация системы управления информационной безопасностью Учреждения

1.1.1. Организация системы управления информационной безопасности

СУИБ Учреждения – часть общей системы управления Учреждения, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения ИБ Учреждения.

Для успешного функционирования СУИБ Учреждения должны быть реализованы следующие процессы:

– определение и уточнение области действия СУИБ и выбор подхода к оценке рисков ИБ.

– определение и уточнение области действия СУИБ должно осуществляться на основе результатов оценки рисков, связанных с основной деятельностью Учреждения, а также оценки правовых рисков деятельности Учреждения.

– анализ и оценка рисков ИБ, варианты обработки рисков ИБ для наиболее критичных информационных активов.

– выбор и уточнение целей ИБ и защитных мер и их обоснование для минимизации рисков ИБ.

– принятие руководством Учреждения остаточных рисков и решения о реализации и эксплуатации/совершенствовании СУИБ. Остаточные риски ИБ должны быть соотнесены с рисками деятельности Учреждения, и оценено их влияние на достижение целей деятельности Учреждения.

1.1.2. Реализация системы управления информационной безопасностью

В СУИБ должны быть реализованы следующие процессы:

– разработка плана обработки рисков ИБ;

– реализация плана обработки рисков ИБ и реализация защитных мер, управление работами и ресурсами, связанными с реализацией СУИБ;

– реализация программ по обучению и осведомленности ИБ;

– обнаружение и реагирование на инциденты безопасности;

– обеспечение непрерывности деятельности и восстановления после прерываний.

На этапе планирования определяется политика и методология управления рисками, а также выполняется оценка рисков, включающая в себя инвентаризацию активов, составление профилей угроз и уязвимостей, оценку эффективности контрмер и потенциального ущерба, определение допустимого уровня остаточных рисков.

На этапе реализации производится обработка рисков и внедрение механизмов контроля, предназначенных для их минимизации. Учреждением принимается одно из четырех решений по каждому идентифицированному риску: проигнорировать, избежать, передать внешней стороне, либо минимизировать. После этого разрабатывается и внедряется план обработки рисков.

На этапе проверки отслеживается функционирование механизмов контроля, контролируются изменения факторов риска (активов, угроз, уязвимостей), проводятся аудиты и выполняются различные контролирующие процедуры.

На этапе действия по результатам непрерывного мониторинга и проводимых проверок, выполняются необходимые корректирующие действия, которые могут включать в себя, в частности, переоценку величины рисков, корректировку политики и методологии управления рисками, а также плана обработки рисков.

1.1.3. Методы оценивания информационных рисков

Оценка информационных рисков Учреждения выполняется по следующим основным этапам:

– идентификация и количественная оценка ИР, значимых для работы Учреждения;

– оценивание возможных угроз;
– оценивание существующих уязвимостей;
– оценивание эффективности средств обеспечения ИБ.

Предполагается, что значимые уязвимые ИР Учреждения подвергаются риску, если по отношению к ним существуют какие-либо угрозы.

При этом информационные риски зависят от:

– показателей ценности ИР;
– вероятности реализации угроз для ресурсов;
– эффективности существующих или планируемых средств обеспечения ИБ.

Цель оценивания рисков состоит в определении характеристик рисков ИС и ее ресурсов. В результате оценки рисков становится возможным выбрать средства, обеспечивающие желаемый уровень ИБ организации.

При оценивании рисков учитываются: ценность ресурсов, значимость угроз и уязвимостей, эффективность существующих и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть определены как количественными методами, например, при определении стоимостных характеристик, так и качественными, например учитывающими штатные или чрезвычайно опасные нештатные воздействия внешней среды.

Возможность реализации угрозы оценивается вероятностью ее реализации в течение заданного отрезка времени для некоторого ресурса Учреждения.

При этом вероятность того, что угроза реализуется, определяется следующими основными показателями:

– привлекательностью ресурса, используется при рассмотрении угрозы от умышленного воздействия со стороны человека;
– возможностью использования ресурса для получения дохода, также используется при рассмотрении угрозы от умышленного воздействия со стороны человека;
– техническими возможностями реализации угрозы, используется при умышленном воздействии со стороны человека;
– степенью легкости, с которой уязвимость может быть использована.

2.8. Политики информационной безопасности

1.1.4. Политика предоставления доступа к информационному ресурсу

1.1.5. Назначение

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к защищаемым ИР Учреждения.

2.8.1.1.Положение политики

К работе с ИР допускаются пользователи, ознакомленные с правилами работы с ИР и ответственностью за их нарушение, а также настоящей политикой.

Каждому сотруднику Учреждения, допущенному к работе с конкретным ИР, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИС.

В случае необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими

сотрудниками при работе в АС Учреждения одного и того же имени пользователя («группового имени») ЗАПРЕЩЕНО.

2.8.1.2.Порядок создания (продления) учетной записи пользователя

Процедура регистрации (создания учетной записи), так же продления срока действия временной учетной записи пользователя для сотрудника Учреждения инициируется заявкой (Приложение № 1).

В заявке указывается:

– должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;

– основание для регистрации учетной записи (номер приказа о принятии на работу в Учреждении или иного договорного документа, определяющего необходимость предоставления сотруднику доступа к ИР Учреждения).

Заявку подписывает начальник кадровой службы подтверждающий, что указанный сотрудник действительно принят в штат Учреждения.

Заявка согласуется с АИБом и передается системному администратору.

Системный администратор рассматривает представленную заявку и совершает необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля и минимальных прав доступа к ресурсам Учреждения.

По окончании регистрации учетной записи пользователя в заявке делается отметка о выполнении задания за подписями исполнителей.

Минимальные права в ИС Учреждения, определенные выше, а также присвоение начального пароля производится АИБом, при согласовании заявки на предоставление (изменение) прав доступа пользователя к ИР.

2.8.1.3.Порядок предоставления (изменения) полномочий пользователя

Процедура регистрации (создания учетной записи), так же продления срока действия временной учетной записи пользователя для сотрудника Учреждения инициируется заявкой (Приложение № 1).

В заявке указывается:

– должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;

– основание для регистрации учетной записи (номер приказа о принятии на работу в Учреждении или иного договорного документа, определяющего необходимость предоставления сотруднику доступа к ИР Учреждения).

Заявку подписывает начальник кадровой службы подтверждающий, что указанный сотрудник действительно принят в штат Учреждения.

Заявка согласуется с АИБом и передается системному администратору.

Системный администратор рассматривает представленную заявку и совершает необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля и минимальных прав доступа к ресурсам Учреждения.

По окончании регистрации учетной записи пользователя в заявке делается отметка о выполнении задания за подписями исполнителей.

Минимальные права в ИС Учреждения, определенные выше, а также присвоение начального пароля производится АИБом, при согласовании заявки на предоставление (изменение) прав доступа пользователя к ИР.

2.8.1.4.Порядок предоставления (изменения) полномочий пользователя

Процедура предоставления (или изменения) прав доступа пользователя к ресурсам Учреждения. инициируется заявкой руководителя структурного подразделения сотрудника (Приложение № 2).

В заявке указывается:

– должность, фамилия, имя и отчество сотрудника;

– имя пользователя (учетной записи) данного сотрудника;

– наименование информационного актива (системы, ресурса), к которому необходим допуск (или изменение полномочий пользователя);

– полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач на конкретных ИР ИС) с указанием разрешенных видов доступа к ресурсу (ролей).

Заявка согласуется с АИБом и передается системному администратору на исполнение.

По окончании внесения изменений в заявке делается отметка о выполнении задания за подписями исполнителей.

2.8.1.5.Порядок удаления учетной записи пользователя

При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение сотрудника) учетная запись должна немедленно блокироваться.

Предпочтительно использовать механизмы автоматического блокирования учетных записей уволенных сотрудников, используя соответствующие ИС. При невозможности автоматического блокирования учетных записей, сотрудникам сопоставляются временные учетные записи (с фиксированным сроком действия), о чем делается отметка в заявке при ее исполнении и в обязательном порядке доводится до инициатора заявки.

Допускается регистрация постоянных учетных записей при отсутствии механизмов автоматической блокировки. В этом случае начальник кадровой службы обязан своевременно подавать заявки на блокирование учетной записи сотрудника (Приложение №3) не позднее, чем за сутки до момента прекращения срока действия полномочий пользователя.

В заявке указывается:

– должность сотрудника, фамилия, имя и отчество сотрудника;

– имя пользователя (учетной записи) данного сотрудника;

– дата прекращения полномочий пользователя.

Заявку подписывает начальник кадровой службы, утверждая тем самым факт прекращения срока действия полномочий пользователя.

АИБ рассматривает представленную заявку и передает заявку на исполнение системному администратору.

По окончании внесения изменений в заявке делается отметка о выполнении задания за подписями исполнителей.

В случае необходимости сохранения персональных документов (профайла пользователя) на АРМ сотрудника, после прекращения срока действия его полномочий, сотрудник (или его непосредственный руководитель) должен своевременно (не позднее, чем за 3 суток до момента прекращения срока действия своих полномочий) подать заявку на блокирование учетной записи пользователя с указанием срока хранения указанной информации. Заявка должна подаваться даже в случае применения механизмов автоматической блокировки учетных записей уволенных сотрудников.

Такая заявка должна быть предварительно согласована с АИБом, и после выполнения действий по блокированию учетной записи передается системному администратору для исполнения требования по сохранению данных.

2.8.1.6.Порядок хранения исполненных заявок

Исполненные заявки передаются АИБу, и хранятся в архиве в течение 5 лет с момента окончания предоставления доступа к ИР Учреждения.

Копии исполненных заявок хранятся у системного администратора.

Они могут впоследствии использоваться:

– для восстановления полномочий пользователей после аварий в ИС Учреждения;

– для контроля правомерности наличия у конкретного пользователя прав доступа к ИР;

– тем или иным ресурсам системы при разборе конфликтных ситуаций;

– для проверки правильности настройки средств разграничения доступа к ресурсам системы.

В случае невозможности исполнения инициатору заявки направляется мотивированный отказ с приложением Заявки.

1.1.6. Политика учетных записей

1.1.7. Назначение

Настоящая политика определяет основные правила присвоения учетных записей пользователям информационных активов Учреждения.

2.8.1.7.Положение политики

Регистрационные учетные записи подразделяются на:

– пользовательские – предназначенные для идентификации/аутентификации пользователей информационных активов Учреждения;

– системные – используемые для нужд операционной системы;

– служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений.

Каждому пользователю информационных активов Учреждения назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

В общем случае запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или организации труда (например, посменное дежурство), использование общей учетной записи должно сопровождаться

отметкой в журнале учета машинного времени, которая должна однозначно идентифицировать текущего владельца учетной записи в каждый момент времени. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.

Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.

Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.

Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.

1.1.8. Политика использования паролей

1.1.9. Назначение

1.1.10. Положения политики

Положения политики закрепляются в «Инструкции по парольной защите в АС».

1.1.11. Политика реализации антивирусной защиты

1.1.12. Назначение

Настоящая Политика определяет основные правила для реализации антивирусной защиты в Учреждении.

2.8.1.8.Положения политики

Положения политики закрепляются в «Инструкции по проведению антивирусного контроля в АС».

1.1.13. Политика защиты автоматизированного рабочего места

1.1.14. Назначение

Настоящая Политика определяет основные правила и требования по защите ПДн и иной КИ Учреждения от неавторизованного доступа, утраты или модификации.

2.8.1.9.Положения политики

Во время работы с КИ должен предотвращаться ее просмотр не допущенными к ней лицами.

При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие КИ, заперты в помещении, шкафу или ящике стола или в сейфе.

Несанкционированное использование печатающих, факсимильных, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа.

Сотрудники получают доступ к ресурсам вычислительной сети после ознакомления с документами, утвержденными стандартами предприятия, (согласно занимаемой должности), а именно с инструкциями по обращению с носителями КИ, «Перечнем сведений конфиденциального характера».

Доступ к компонентам операционной системы и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставлено только АИБу. Конечным пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их должностных обязанностей.

Доступ к информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.

Пользователям запрещается устанавливать неавторизованные программы на компьютеры.

Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неавторизованных программ.

Техническое обслуживание должно осуществляться только на основании обращения пользователя к системному администратору.

Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.

Дистанционное техническое обслуживание должно осуществляться только со специально выделенных АРМ, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться.

При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

Копирование КИ и временное изъятие носителей КИ (в том числе в составе АРМ) допускаются только с санкции пользователя. В случае изъятия носителей, содержащих КИ, пользователь имеет право присутствовать при дальнейшем проведении работ.

ПО должно устанавливаться со специальных ресурсов или съемных носителей и в соответствии с лицензионным соглашением с его правообладателем.

Конфигурации устанавливаемых рабочих станций должны быть стандартизованы, а процессы установки, настройки и ввода в эксплуатацию - регламентированы.

АРМ, на которых предполагается обрабатывать КИ, должны быть закреплены за соответствующими сотрудниками Учреждения. Запрещается использование указанных АРМ другими пользователями без согласования с АИБом Учреждения. При передаче указанного АРМ другому пользователю, должна производится гарантированная очистка диска (форматирование).

Системный администратор вправе отказать в устранении проблемы, вызванной наличием на рабочем месте ПО или оборудования, установленного или настроенного пользователем в обход действующей процедуры.

2.9. Порядок сопровождения информационной системы Учреждения

Обеспечение ИБ ИС на стадиях жизненного цикла ИБ ИС должна обеспечиваться на всех стадиях ЖЦ ИС, автоматизирующих технологические процессы, с учетом всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений организации). Разработка технических заданий, проектирование, создание, тестирование, приемка средств и систем

защиты ИС проводится при участии АИБа и системного администратора. Порядок разработки и внедрения ИС должен быть регламентирован и контролироваться.

При разработке ИС необходимо придерживаться требований и методических указаний, определенных стандартами, входящими в группу ГОСТ 34.ххх «Стандарты информационной технологии».

Ввод в действие, эксплуатация, снятие с эксплуатации ИС в части вопросов ИБ должны осуществляться при участии АИБа.

На стадиях, связанных с разработкой ИС (определение требований заинтересованных сторон, анализ требований, архитектурное проектирование, реализация, интеграция и верификация, поставка, ввод в действие), разработчиком должна быть обеспечена защита от угроз:

– неверной формулировки требований к ИС;

– выбора неадекватной модели ЖЦ ИС, в том числе неадекватного выбора процессов ЖЦ и вовлеченных в них участников;

– принятия неверных проектных решений;

– внесения разработчиком дефектов на уровне архитектурных решений;

– внесения разработчиком недокументированных возможностей в ИС;

– неадекватной (неполной, противоречивой, некорректной и пр.) реализации требований к ИС;

– разработки некачественной документации;

– сборки ИС разработчиком/производителем с нарушением требований, что приводит к появлению недокументированных возможностей в ИС либо к неадекватной реализации требований;

– неверного конфигурирования ИС;

– приемки ИС, не отвечающей требованиям заказчика;

– внесения недокументированных возможностей в ИС в процессе проведения приемочных испытаний посредством недокументированных возможностей функциональных тестов и тестов ИБ.

Привлекаемые для разработки средств и систем защиты ИС на договорной основе специализированные организации должны иметь лицензии на данный вид деятельности в соответствии с законодательством РФ.

При приобретении готовых ИС и их компонентов разработчиком должна быть предоставлена документация, содержащая, в том числе, описание защитных мер, предпринятых разработчиком в отношении угроз информационной безопасности.

Также разработчиком должна быть представлена документация, содержащая описание защитных мер, предпринятых разработчиком ИС и их компонентов относительно безопасности разработки, безопасности поставки, эксплуатации, поддержки жизненного цикла, включая описание модели жизненного цикла, оценки уязвимости. Данная документация может быть представлена в рамках декларации о соответствии или быть результатом оценки соответствия изделия, проведенной в рамках соответствующей системы оценки.

В договор (контракт) о поставке ИС и их компонентов рекомендуется включать положения по сопровождению поставляемых изделий на весь срок их службы. В случае невозможности включения в договор (контракт) указанных требований к разработчику должна быть рассмотрена возможность приобретения полного комплекта рабочей

конструкторской документации на изделие, обеспечивающее возможность сопровождения ИС и их компонентов без участия разработчика. Если оба указанных варианта неприемлемы, например, вследствие высокой стоимости, руководство Учреждения, должно обеспечить анализ влияния угрозы невозможности сопровождения ИС и их компонентов на обеспечение непрерывности работы.

На стадии эксплуатации должна быть обеспечена защита от следующих угроз:

– умышленное несанкционированное раскрытие, модификация или уничтожение информации;

– неумышленная модификация или уничтожение информации;

– недоставка или ошибочная доставка информации;

– отказ в обслуживании или ухудшение обслуживания.

Кроме этого, актуальной является угроза отказа от авторства сообщения. На стадии сопровождения должна быть обеспечена защита от угроз:

– внесения изменений в ИС, приводящих к нарушению ее функциональности либо к появлению недокументированных возможностей;

– невнесения разработчиком/поставщиком изменений, необходимых для поддержки правильного функционирования и правильного состояния ИС.

На стадии снятия с эксплуатации должно быть обеспечено удаление информации, несанкционированное использование которой может нанести ущерб Учреждению, и информации, используемой средствами обеспечения ИБ, из постоянной памяти ИС или с внешних носителей.

Требования ИБ должны включаться во все договора и контракты на проведение работ или оказание услуг на всех стадиях ЖЦ ИС.

1.1.15. Профилактика нарушений политик информационной безопасности

Под профилактикой нарушений политик ИБ понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений ИБ в Учреждении и проведение разъяснительной работы по ИБ среди пользователей.

Проведение в ИС Учреждения регламентных работ по защите информации предполагает выполнение процедур контрольного тестирования (проверки) функций СЗИ, что гарантирует ее работоспособность с точностью до периода тестирования. Контрольное тестирование функций СЗИ может быть частичным или полным и должно проводиться с установленной в ИС Учреждения степенью периодичности.

Задача предупреждения в ИС Учреждения возможных нарушений ИБ решается по мере наступления следующих событий:

– включение в состав ИС Учреждения новых программных и технических средств (новых рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС Учреждения;

– изменение конфигурации программных и технических средств ИС (изменение конфигурации ПО рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС Учреждения;

– при появлении сведений о выявленных уязвимых местах в составе операционных систем и/или ПО технических средств, используемых в ИС Учреждения.

АИБ (возможно, при помощи сторонней организации специализирующейся в области информационной безопасности) собирает и анализирует информацию о

выявленных уязвимых местах в составе операционных систем и/или ПО относительно ИС Учреждения. Источниками подобного рода сведений могут служить официальные издания и публикации различных компаний, Учрежденииинных объединений и других организаций, специализирующихся в области защиты информации.

АИБ (возможно, при помощи сторонней организации, специализирующейся в области ИБ) организовывает периодическую проверку СЗИ ИС Учреждения путем моделирования возможных попыток осуществления НСД к защищаемым ИР.

Для решения задач контроля защищенности ИС используются инструментальные средства для тестирования реализованных в составе СЗИ ИС Учреждения средств и функций защиты. По результатам профилактических работ, проводимых в ИС, необходимо сделать соответствующие записи в «Журнале проверки исправности и технического обслуживания».

Плановая разъяснительная работа по правилам настоящих политик, а также инструктаж сотрудников Учреждения по соблюдению требований нормативных и регламентных документов по ИБ, принятых в Учреждении, проводится АИБом ежегодно.

Внеплановая разъяснительная работа по правилам настоящих политик, а также инструктаж сотрудников Учреждения по соблюдению требований нормативных и регламентных документов по ИБ, принятых в Учреждении, проводится при пересмотре настоящих политик, при возникновении инцидента нарушения правил настоящих политик.

Прием на работу новых сотрудников должен сопровождаться ознакомлением их с правилами и требованиями настоящих политик.

1.1.16. Ликвидация последствий нарушения политик информационной безопасности

АИБ, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС, должен своевременно обнаруживать нарушения ИБ, факты осуществления НСД к защищаемым ИР и предпринимать меры по их локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения ИБ или осуществления НСД к защищаемым ИР ИС рекомендуется уведомить АИБа и/или ответственного по вопросам информационных технологий Учреждения, и далее следовать их указаниям.

Действия АИБа и системного администратора при признаках нарушения политик информационной безопасности регламентируются следующими внутренними документами:

- Инструкцией пользователя автоматизированной системы;
- Политикой информационной безопасности;
- Должностными обязанностями администратора информационной безопасности;
- Должностными обязанностями системного администратора.

После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС, а также зарегистрировать факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

1.1.17. Ответственность нарушителей Политик безопасности

Ответственность за выполнение правил ПБ несет каждый сотрудник Учреждения в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования ПБ Учреждения, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный Учреждению в результате нарушения ими правил политики ИБ (Ст. 238 Трудового кодекса РФ).

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, сотрудники Учреждения несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.

3. Регулирующие законодательные нормативные документы

При организации и обеспечении работ по ИБ сотрудники Учреждения должны руководствоваться следующими законодательными нормативными документами:

3.1. Основополагающие нормативные документы

К основополагающим нормативным документам относятся:

– Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г.);

– Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов (разработана во исполнение Указа Президента Российской Федерации от 1 июля 1994 г. № 1390 «О совершенствовании информационно-телекоммуникационного обеспечения органов государственной власти и порядке их взаимодействия при реализации государственной политики в сфере информатизации»);

– Стратегия национальной безопасности Российской Федерации (утверждена Указом Президента РФ от 31.12.2015 № 683);

– Доктрина информационной безопасности Российской Федерации (утверждена Указ Президента РФ от 05.12.2016 № 646).

3.2. Законы Российской Федерации

– Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности» (с изменениями от 05.10.2015 г.);

– Гражданский кодекс Российской Федерации часть первая от 30 ноября 1994 г. № 52-ФЗ, часть вторая от 26 января 1996 г. № 14-ФЗ, часть третья от 26 ноября 2001 г. № 146-ФЗ и часть четвертая от 18 декабря 2006 г. № 230-ФЗ;

– Закон Российской Федерации от 27 ноября 1992 г. № 4015-I «Об организации страхового дела в Российской Федерации» (с изменениями от 03.07.2016 г.);

– Федеральный закон от 21 декабря 1994 г. № 69-ФЗ «О пожарной безопасности» (с изменениями от 23.06.2016 г.)

– Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (с изменениями от 06.07.2016г.);

– Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (с изменениями от 23.06.2016 г.);

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями от 03.07.2016 г.);

– Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» (с изменениями от 08.03.2015 г.);

– Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» (с изменениями от 06.07.2016 г.);

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями от 06.07.2016 г.);

– Федеральный закон от 9 января 1996 г. № 2-ФЗ «О внесении изменений и дополнений в Закон Российской Федерации «О защите прав потребителей» и Кодекс РСФСР об административных правонарушениях» (с изменениями от 30 декабря 2001 г., 25 октября 2007 г., 3 июня 2009 г.);

– Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ (с изменениями от 03.07.2016 г);

– Федеральный закон от 13 декабря 1996 г. № 150-ФЗ «Об оружии» (с изменениями от 06.07.2016 г.);

– Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» (с изменениями от 05.04.2016 г.);

– Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» (с изменениями от 30.12.2015 г.).

3.3. Указы и распоряжения президента Российской Федерации

– Указ Президента Российской Федерации от 7 октября 1993 г. № 1607 «О государственной политике в области охраны авторского права и смежных прав»;

– Указ Президента Российской Федерации от 31 декабря 1993 г. № 2334 «О дополнительных гарантиях прав граждан на информацию» (с изменениями от 17 января 1997 г., 1 сентября 2000 г.);

– Указ Президента Российской Федерации от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации» (с изменениями от 26 июля 1995 г., 17 января, 9 июля 1997 г.);

– Указ Президента Российской Федерации от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» (с изменениями от 25 июля 2000 г.);

– Указ Президента Российской Федерации от 3 июля 1995 г. № 662 «О мерах по формированию общероссийской телекоммуникационной системы и обеспечению прав собственников при хранении ценных бумаг и расчетах на фондовом рынке Российской Федерации» (с изменениями от 16 августа 1995 г., 4 января 1996 г., 28 мая 1997 г., 29 ноября 2004 г., 16 октября 2010 г.);

– Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне» (с изменениями от 10.10.2016 г.);

– Указ Президента Российской Федерации от 9 января 1996 г. № 21 «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации» (с изменениями от 30 декабря 2000 г.);

– Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (с изменениями от 31.12.2015 г.);

– Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями от 13.07.2015 г);

– Распоряжение Президента Российской Федерации от 16 апреля 2005 г. № 151-рп «О перечне должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне» (с изменениями, от 10.10.2016 г.).

3.4. Постановления и распоряжения правительства Российской Федерации

–Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»;

–Постановление Правительства Российской Федерации от 15 апреля 1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» (в редакции от ред. от 24.12.2014);

–Постановление Правительства РФ от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»;

–Постановление Правительства РФ от 03.03.2012 № 171 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»;

–Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации» (ред. от 21.04.2010);

– Постановление Правительства Российской Федерации от 4 сентября 1995 г. № 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» (в редакции Постановлений Правительства РФ от 15.01.2008 г., от 22.05.2008 г., от 18.03.2016г.);

– Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»;

– Постановление Правительства Российской Федерации от 1 июля 1996 г. № 770 «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности,

связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности» (с изменениями от 15 июля 2002 г.);

– Постановление Правительства Российской Федерации от 2 августа 1997 г. № 973 «Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам (в редакции от 18.03.2016);

3.5. Нормативные и руководящие документы Федеральных служб Российской Федерации

– Решение Гостехкомиссии России от 21 октября 1997 г. № 61 «О защите информации при вхождении России в международную информационную систему «Интернет»;

– Приказ ФСТЭК России от 12.07.2012 №83 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации» (в редакции от 20.05.2015 г.);

– Приказ ФСБ Российской Федерации от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

– Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР) (утверждено решением Гостехкомиссии России от 23 мая 1997 г. № 55-с);

– Постановление Госстандарта Российской Федерации от 21 сентября 1994 г. № 15 «Об утверждении «Порядка проведения сертификации продукции в Российской Федерации» (с изменениями от 25 июля 1996 г., 11 июля 2002 г.);

– Постановление Госстандарта Российской Федерации от 10 мая 2000 г. № 26 «Об утверждении Правил по проведению сертификации в Российской Федерации» (с изменениями от 5 июля 2002 г.);

– Положение о сертификации средств защиты информации по требованиям безопасности информации (утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995 г. № 199);

– Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.);

– Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации (утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации т 5 января 1996 г. № 3);

– Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации (утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);

– Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах

вычислительной техники (утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);

– Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);

– Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);

– Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения (утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.);

– Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.);

– Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.);

– Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114);

– Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (введен в действие Приказом Гостехкомиссии России от 19.06.02 г. № 187);

– Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации, Гостехкомиссия России, Москва, 2002;

– Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации, Гостехкомиссия России, Москва, 2002;

– Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам, Гостехкомиссия России, Москва, 2002;

– Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах, Гостехкомиссия России, Москва, 2002;

– Нормативно-методический документ. Специальные требования и рекомендации по технической защите конфиденциальной информации (утвержден приказом Гостехкомиссии России от 30 августа 2002 г. № 282);

3.6. Государственные стандарты

– ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и

хранение» (утвержден постановлением Госстандарта СССР от 28 июня 1984 г. № 2206, с изменениями от июня 1987 г., ноября 1988 г., декабря 1990 г.);

– ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» (утвержден постановлением Госстандарта СССР от 24 марта 1989 г. № 661);

– ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» (принят постановлением Госстандарта России от 9 февраля 1995 г. № 49);

– ГОСТ Р 50752-95 «Информационная технология. Защита информации от утечки за счёт побочных электромагнитных излучений при её обработке средствами вычислительной техники. Методы испытаний», Госстандарт России, 1995 г.;

– ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство» (введен в действие постановлением Госстандарта России от 14 июля 1998 г. № 295);

– ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения», Госстандарт России, 2000 г.;

– ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования», Госстандарт России, 2000 г.;

– ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью» (принят постановлением Госстандарта России от 29 декабря 2005 г. № 447-ст);

Приложения

Перечень приложений к политике информационной безопасности

НОМЕР ПРИЛОЖЕНИЯ	НАИМЕНОВАНИЕ ПРИЛОЖЕНИЯ	КРАТКОЕ ОПИСАНИЕ СОДЕРЖАНИЯ	ПРИМЕЧАНИЕ
1	Форма заявления на создание учетной записи пользователя	Содержит форму заявления, которое должен написать руководитель пользователя для создания пользовательской учетной записи в ИС Учреждения	Включено в настоящий документ
2	Форма заявления на создание и изменение полномочий пользователю	Содержит форму заявления, оформляемого руководителем пользователя для наделения пользователя новыми полномочиями для работы с информационными ресурсами ИС Учреждения	Включено в настоящий документ
3	Форма заявления на блокировку учетной записи пользователя	Содержит форму заявления, оформляемого руководителем пользователя для блокирования учетной записи пользователя	Включено в настоящий документ

Приложение 1

Форма заявления на создание учетной записи пользователя

СОГЛАСОВАНО
Специалист по кадрам «___» _____ 201_ г.
(для штатных сотрудников)

Администратор информационной безопасности «___» _____ 201_ г.

ЗАЯВЛЕНИЕ № _____
На создание (продление) учетной записи пользователя

Прошу создать (продлить) учетную запись пользователя:

Наименование структурного подразделения	
Ф.И.О. сотрудника, должность, телефон	
Ф.И.О. непосредственного руководителя, должность, телефон	

Сотрудник приступает к работе с: «___» _____ 20__г. по «___» _____ 20__г.
указывается при необходимости

Обоснование служебной
необходимости:_____
_____
_____
_____
_____

_____ «___» _____ 20__г.
фамилия И.О. руководителя подразделения подпись дата

С правилами работы в информационной системе КГБПОУ «Барнаульский государственный педагогический колледж» ознакомлен(а)

_____ _____ «___» _____ 20__г.
фамилия И.О. сотрудника подпись дата

Выполнено: _____ _____
назначенное имя пользователя адрес почты

Ответственный за техническое обслуживание _____ _____ Системное Время:
____чч____мм
подпись фамилия И.О.

Дата: «___» _____ 201_ г.

Приложение 2

Форма заявления на изменение полномочий

СОГЛАСОВАНО

Администратор информационной безопасности «___» _____ 201_ г.

ЗАЯВЛЕНИЕ № _____
На изменение полномочий пользователю

Прошу изменить полномочия по работе с информационным ресурсом:

Наименование структурного подразделения	
Ф.И.О. сотрудника, должность, телефон	
Имя в системе (указывается если есть)	
Ф.И.О. непосредственного руководителя, должность, телефон	
Наименование информационного ресурса	
Старые полномочия (если были)	
Новые полномочия	

Изменения вступают в силу с: «___» _____ 20__г. по «___» _____ 20__г.
(указывается при необходимости)

Обоснование служебной необходимости:_____
_____
_____

_____ _____ «___» _____ 20__г.
фамилия И.О. руководителя подразделения подпись дата

С правилами работы в информационной системе КГБПОУ «Барнаульский государственный педагогический колледж» ознакомлен(на)
_____ _____ «___» _____ 20__г.
фамилия И.О. сотрудника подпись дата

Выполнено:
_____
назначенное имя пользователя, описание выполненных действий

Ответственный за техническое обслуживание _____ _____ Системное Время: ____чч____мм
подпись фамилия И.О.

Дата: «___» _____ 20__г.

Приложение 3

Форма заявления на блокировку учетной записи

Специалист по кадрам «___» _____ 201_ г.
(для штатных сотрудников)

Администратор информационной безопасности «___» _____ 201_ г.

ЗАЯВЛЕНИЕ № _____
На блокировку учетной записи пользователя

Прошу заблокировать учетную запись пользователя:

Наименование структурного подразделения	
Ф.И.О. сотрудника, должность, телефон	
Имя в системе	
Ф.И.О. непосредственного руководителя, должность, телефон	

Срок действия полномочий прекратить с: «___» _____ 20__г.

Обоснование
блокировки:_____
_____
_____

_____ _____ «___» _____ 20__г.
фамилия И.О. руководителя подразделения подпись дата

С гарантированным хранением данных в течении
_____
указывается срок хранения данных пользователя

Пользователь блокирован

Ответственный за техническое обслуживание _____ _____ Системное Время:
____чч____мм
подпись фамилия И.О.

Дата: «___» _____ 201_ г.