УТВЕРЖДАЮ
Глава администрации
Железнодорожного района
г.Барнаула

_____М.Н.Звягинцев
"11" 05 20 18 г.

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АДМИНИСТРАЦИИ ЖЕЛЕЗНОДОРОЖНОГО РАЙОНА
ГОРОДА БАРНАУЛА

1. Вводные положения

1.1. Введение

Политика информационной безопасности администрации Железнодорожного района города Барнаула (далее – Администрация) определяет цели и задачи системы обеспечения информационной безопасности (ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Администрация в своей деятельности.

1.2. Цели

Основными целями политики информационной безопасности Администрации являются защита информации организации и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в его Уставе.

Общее руководство обеспечением ИБ Администрации осуществляет заместитель главы администрации, руководитель аппарата администрации. Ответственность за организацию мероприятий по обеспечению ИБ несет заведующий отделом информатизации, контроль за соблюдением требований ИБ осуществляет заведующий отделом информатизации. Ответственность за функционирование автоматизированной системы Администрации несет заведующий отделом информатизации.

Руководители органов Администрации ответственны за обеспечение выполнения требований ИБ в своих органах.

Сотрудники обязаны соблюдать порядок обращения со сведениями ограниченного доступа, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других документов ИБ.

1.3. Задачи

Политика информационной безопасности Администрации 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 Администрации обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне Администрации), 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 информационной безопасности в Администрации 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 система управления ИБ является наиболее правильным и эффективным способом добиться минимизации рисков нарушения ИБ для Администрации. 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 системы управления информационной безопасностью в Администрации;

– определение Политик информационной безопасности Администрации, а именно:

– Политика реализации антивирусной защиты;

– Политика учетных записей;

– Политика предоставления доступа к информационному ресурсу;

– Политика использования информационного ресурса в рамках существующих информационных систем;

– Политика использования паролей;

– Политика защиты АРМ;

– Политика работы с носителями информации ограниченного доступа;

– определение порядка сопровождения ИС Администрации.

1.4. Область действия

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

1.5. Период действия и порядок внесения изменений

Настоящая политика вводится в действие после утверждения ее главой администрации Железнодорожного района города Барнаула.

Политика признается утратившей силу после отмены главой администрации Железнодорожного района ее утверждения.

Изменения в политику вносятся по решению главы администрации Железнодорожного района. Инициатором внесения изменений в политику информационной безопасности является заведующий отделом информатизации, который выполняет функции администратора информационной безопасности.

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.

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 Администрации;

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

Ответственным за актуализацию политики информационной безопасности (плановую и внеплановую) является заведующий отделом информатизации, который выполняет функции администратора информационной безопасности.

Контроль за исполнением требований настоящей политики и поддержанием ее в актуальном состоянии возлагается на заведующего отделом информатизации, который выполняет функции администратора информационной безопасности.

2. Термины и определения

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

Администратор информационной безопасности – заведующий отделом информатизации, осуществляющий контроль за обеспечением защиты информации в ЛВС, а также осуществляющий организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Администратор сети – заведующий отделом информатизации, осуществляющий непосредственную организацию и выполнение работ по созданию (модернизации), техническому обслуживанию и управлению (администрированию) информационной управляющей ЛВС, включая технические аспекты информационной безопасности.

Актив – что-либо, что имеет ценность для организации.

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 самой организацией (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.

Внутренняя сеть – внутренний участок корпоративной сети, отделенный от внешней сети (сети Интернет) и демилитаризованной зоны (DMZ) межсетевым экраном. Внутренняя сеть объединяет производственные, тестовые, административные сети и сети разработчиков.

Доступ к информации – возможность получения информации и ее использования.

Доступность – доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

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

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 организации, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Информационная безопасность – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов организации 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 организации.

Информационная среда – совокупность информационно-телекоммуникационной системы Администрации, процессов, источников и потребителей информации, обслуживающего персонала и пользователей информационных систем, обеспечивающего автоматизацию производственных процессов Администрации.

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

Информационно-телекоммуникационная система – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники, а также информационные системы, обеспечивающие автоматизацию процессов Администрации, и средства защиты информации.

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, используемая в рабочих процессах Администрации.

Инфраструктура открытых ключей (ИОК, PKI) – технологическая инфраструктура и сервисы, обеспечивающие безопасность

информационных и коммуникационных систем на основе использования криптографических алгоритмов и сертификатов ключей подписей.

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

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

Код аутентификации электронного сообщения – данные, используемые для установления подлинности и контроля целостности электронного сообщения.

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 санкционированных пользователей.

Корпоративная сеть – объединение информационных систем, компьютерного, телекоммуникационного и офисного оборудования всех подразделений Администрации, посредством их подключения к единой компьютерной сети передачи данных с использованием различных физических и логических каналов связи.

Критичная информация – информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование органов Администрации, нанести Администрации материальный или иной ущерб.

Криптопровайдер – программный или программно-аппаратный модуль, реализующий алгоритмы шифрования.

Локальная вычислительная сеть (ЛВС) – 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 (МЭ) – программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав корпоративной сети, а также между корпоративной сетью и внешними сетями (сетью Интернет).

Менеджмент риска – скоординированные действия по руководству и управлению учреждением в отношении риска.

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 организации, информационные услуги организации и пр.

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

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

Операционная система – системная программа, осуществляющая взаимодействие пользователя и прикладных программ с аппаратной частью ЭВМ.

Остаточный риск – риск, остающийся после обработки риска.

Владелец информационных активов – сотрудник Администрации, получивший на основании соответствующего распорядительного документа права обладателя информации, обрабатываемой в информационной системе.

Оценивание риска – процесс сравнения оцененного риска с данными критериями риска для определения значимости риска.

Оценка риска – общий процесс анализа риска и оценивания риска.

Пароль – идентификатор субъекта доступа, который является его (субъекта) секретом.

Периметральное средство защиты информации (СЗИ) – шлюз информационной безопасности, обеспечивающий межсетевое экранирование и защиту данных, пересылаемых по открытым каналам связи (шифрование), а так же фильтрацию вредоносного ПО и блокирование внешних атак.

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

Принятие риска – решение принять риск.

Программное обеспечение – совокупность системных и 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.

Сервер – выделенный компьютер, имеющий разделяемые ресурсы, выполняющий определенный перечень задач и предоставляющий пользователям ЛВС ряд сервисов.

Сетевые (информационные) сервисы – сетевые приложения, предоставляющие различные виды сервисов для внутренних и внешних пользователей корпоративной сети, включая DNS, FTP, HTTP, Telnet, и другие.

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.

Системный администратор – сотрудник организации, занимающийся сопровождением автоматизированных систем, отвечающий за функционирование локальной сети организации и ПК.

Список контроля доступа (ACL) – 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 производства, 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).

Орган администрации – орган администрации с самостоятельными функциями, задачами и ответственностью.

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 организации при реализации угроз в информационной сфере.

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

ЭВМ – электронно-вычислительная машина, персональный компьютер.

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.

3. Обозначения и сокращения

АРМ – Автоматизированное рабочее место
АС – Автоматизированная система
БД – База данных
ЗИ – Защита информации
ИБ – Информационная безопасность
ИОК – Инфраструктура открытых ключей
ИС – Информационная система
ИТС – Информационно-телекоммуникационная система
КЗ – Контролируемая зона
МЭ – Межсетевой экран
НСД – Несанкционированный доступ
ОС – Операционная система
ПБ – Политики безопасности
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

4. Политики информационной безопасности администрации Железнодорожного района города Барнаула

4.1. Назначение политик информационной безопасности

Политики информационной безопасности Администрации – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в Администрации.

Под политиками безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политики информационной безопасности относятся к административным мерам обеспечения информационной безопасности и определяют стратегию Администрации в области ИБ.

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

Все документально оформленные решения, формирующие Политики, должны быть утверждены руководством.

4.2. Основные принципы обеспечения ИБ

Основными принципами обеспечения ИБ являются следующие:

– Постоянный и всесторонний анализ информационного пространства организации с целью выявления уязвимостей информационных активов.

– Своевременное обнаружение проблем, потенциально способных повлиять на ИБ организации, 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 организации, а также повышать трудоемкость технологических процессов обработки информации.

– Контроль эффективности принимаемых защитных мер.

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

4.3. Соответствие ПБ действующему законодательству

Правовую основу политик составляют законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, Администрации 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.

4.4. Ответственность за реализацию политики информационной безопасности

Ответственность за разработку мер и контроль обеспечения защиты информации несёт заведующий отделом информатизации.

Ответственность за реализацию политик возлагается:

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

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

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

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

Организация обучения сотрудников Администрации в области информационной безопасности возлагается на заведующего отделом информатизации. Подписи сотрудников об ознакомлении заносятся в Журнал проведения инструктажа по информационной безопасности. Обучение сотрудников Администрации правилам обращения с информацией ограниченного доступа, проводится путем:

– проведения заведующим отделом информатизации инструктивных занятий с сотрудниками, принимаемыми на работу в Администрацию;

– самостоятельного изучения сотрудниками внутренних нормативных документов Администрации.

Допуск персонала к работе с информационными ресурсами Администрации осуществляется только после его ознакомления с

настоящими политиками, а также после ознакомления пользователей с Инструкцией по работе пользователей в АС Администрации, а так же иными инструкциями пользователей отдельных информационных систем. Согласие на соблюдение правил и требований настоящих политик подтверждается подписями сотрудников в Журнале проведения инструктажа по информационной безопасности.

Допуск персонала к работе с информацией ограниченного доступа Администрации осуществляется после ознакомления с Инструкциями по обращению с носителями информации ограниченного распространения. Правила допуска к работе с информационными ресурсами лиц, не являющихся сотрудниками Администрации, определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

4.6. Защищаемые информационные ресурсы администрации Железнодорожного района города Барнаула

Различаются следующие категории информационных ресурсов, подлежащих защите в Администрации:

Информация ограниченного доступа (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 17.11.2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», предусмотренная Перечнем сведений конфиденциального характера.

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

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

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

Конфиденциальная информация представляет собой сведения ограниченного доступа, 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.

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

Для этого в Администрации выполняются следующие мероприятия:

– определяется порядок работы с документами, носителями и др., содержащими сведения ограниченного распространения;

– устанавливается круг лиц и порядок доступа к подобной информации;

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

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

Подписка о неразглашении конфиденциальной информации подписывается при заключении трудового договора, который подписывается всеми сотрудниками организации при приеме на работу в Администрации. Защита информации ограниченного доступа, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых Администрацией с другими организациями. Персональные данные сотрудника организации – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника.

Согласно Ст.86 п.7 Трудового кодекса РФ защита персональных данных 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 персональных данных сотрудника работодатель должен соблюдать следующие требования:

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

– разрешать доступ к персональным данным 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 персональных данных сотрудника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

4.7. Организация системы управления информационной безопасностью администрации Железнодорожного района города Барнаула

4.7.1. Организация системы управления ИБ

Система управления информационной безопасности Администрации (СУИБ) предназначена для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности Администрации.

Для успешного функционирования СУИБ Администрации 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 Администрации, а также оценки репутационных и правовых рисков деятельности Администрации;
- анализ и оценка рисков ИБ, варианты обработки рисков ИБ для наиболее критичных информационных активов и производственных процессов.
- выбор и уточнение целей ИБ и защитных мер и их обоснование для минимизации рисков ИБ.
- принятие руководством Администрации остаточных рисков и решения о реализации и эксплуатации/совершенствовании СУИБ. Остаточные риски ИБ должны быть соотнесены с рисками деятельности Администрации и оценено их влияние на достижение целей деятельности Администрации.

4.7.2. Реализация системы управления ИБ

В системе управления ИБ 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, Администрацией 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.

4.7.3. Методы оценивания информационных рисков

Оценка информационных рисков Администрации выполняется по следующим основным этапам:

– идентификация и количественная оценка информационных ресурсов, значимых для работы Администрации;

– оценивание возможных угроз;

– оценивание существующих уязвимостей;

– оценивание эффективности средств обеспечения информационной безопасности.

Предполагается, что значимые для производственного процесса уязвимые информационные ресурсы Администрации подвергаются риску, если по отношению к ним существуют какие-либо угрозы.

При этом информационные риски зависят от:

– показателей ценности информационных ресурсов;

– вероятности реализации угроз для ресурсов;

– эффективности существующих или планируемых средств обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков корпоративной информационной системы и ее ресурсов. В результате оценки рисков становится возможным выбрать средства,

обеспечивающие желаемый уровень информационной безопасности 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 Администрации.

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.

4.8. Политики информационной безопасности

4.8.1. Политика предоставления доступа к информационному ресурсу

4.8.1.1. Назначение

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к информационным ресурсам Администрации.

4.8.1.2. Положение политики

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

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

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

в Администрации одного и того же имени пользователя («группового имени») ЗАПРЕЩЕНО.

4.8.1.3. Порядок создания (продления) учетной записи пользователя

Процедура регистрации (создания учетной записи), так же продления срока действия временной учетной записи пользователя для сотрудника Администрации инициируется заявкой руководителя органа администрации, в котором работает данный сотрудник (Приложение № 1).

В заявке указывается:

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

– основание для регистрации учетной записи (номер распоряжения о принятии на работу в Администрацию или иного договорного документа, определяющего необходимость предоставления сотруднику доступа к информационным ресурсам Администрации).

Заявку подписывает руководитель органа администрации подтверждающий, что указанный сотрудник действительно принят в штат.

Заявка передается заведующему отделом информатизации.

Заведующий отделом информатизации рассматривает представленную заявку и совершает необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля и минимальных прав доступа к сетевым ресурсам Администрации, таких как право регистрации на АРМ сотрудника и пользования корпоративной электронной почтой.

По окончании регистрации учетной записи пользователя в заявке делается отметка о выполнении задания за подписью исполнителя.

Минимальные права в ИС Администрации, определенные выше, а также присвоение начального пароля производится заведующим отделом информатизации, при согласовании заявки на предоставление (изменение) прав доступа пользователя к информационным ресурсам.

4.8.1.4. Порядок предоставления (изменения) полномочий пользователя

Процедура предоставления (или изменения) прав доступа пользователя к ресурсам Администрации инициируется заявкой 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 информационных ресурсах ИС) с указанием разрешенных видов доступа к ресурсу (ролей).

Заявку подписывает руководитель органа администрации, в котором числится сотрудник согласно штатному расписанию, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных задач ресурсам ИС Администрации.

Заведующий отделом информатизации рассматривают представленную заявку и вносит необходимые изменения в списки полномочий пользователей соответствующих информационных ресурсов.

По окончании внесения изменений в заявке делается отметка о выполнении задания за подписью исполнителя.

4.8.1.5. 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.

Допускается регистрация постоянных учетных записей при отсутствии механизмов автоматической блокировки. В этом случае руководителю органа администрации, в котором числится такой сотрудник согласно штатному расписанию, вменяется в обязанность 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 руководитель органа администрации, утверждая тем самым факт прекращения срока действия полномочий пользователя.

Заведующий отделом информатизации рассматривает представленную заявку и производит блокировку учетной записи пользователя.

По окончании внесения изменений в заявке делается отметка о выполнении задания за подписью исполнителя.

В случае производственной необходимости сохранения персональных документов (профайла пользователя) на АРМ сотрудника Администрации после прекращения срока действия его полномочий руководитель органа администрации должен своевременно (не позднее, чем за 3 суток до момента прекращения срока действия полномочий пользователя) 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 передается заведующему отделом информатизации для исполнения требования по сохранению данных.

4.8.1.6. Порядок хранения исполненных заявок

Исполненные заявки хранятся в архиве органа администрации в течение 1 года с момента окончания предоставления доступа к информационному ресурсу Администрации.

Копии исполненных заявок хранятся у заведующего отделом информатизации.

Они могут впоследствии использоваться:

– для восстановления полномочий пользователей после аварий в ИС Администрации;

– для контроля правомерности наличия у конкретного пользователя прав доступа к информационному ресурсу

– тем или иным ресурсам системы при разборе конфликтных ситуаций;

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

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

4.8.2. Политика учетных записей

4.8.2.1. Назначение

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

4.8.2.2. Положение политики

Регистрационные учетные записи подразделяются на:

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

– системные – используемые для нужд операционной системы;

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

Каждому пользователю информационных активов Администрации 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 событий операционной системы, 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.

4.8.3. Политика использования паролей

4.8.3.1. Назначение

Настоящая политика определяет основные правила обращения с паролями, используемыми для доступа к информационным активам Администрации.

4.8.3.2. Положения политики

Положения политики закрепляются в Инструкции по организации парольной защиты в АС.

4.8.4. Политика реализации антивирусной защиты

4.8.4.1. Назначение

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

4.8.4.2. Положения политики

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

4.8.5. Политика защиты АРМ

4.8.5.1. Назначение

Настоящая Политика определяет основные правила и требования по защите информации ограниченного доступа Администрации от неавторизованного доступа, утраты или модификации.

4.8.5.2. Положения политики

Во время работы с информацией ограниченного доступа должен предотвращаться ее просмотр не допущенными к ней лицами.

При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие информацию ограниченного доступа, 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, регулирующими защиту персональных данных и утвержденными руководством Администрации согласно занимаемой должности.

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

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

Пользователям запрещается устанавливать программное обеспечение на компьютеры без согласования с заведующим отделом информатизации.

Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неразрешенного программного обеспечения.

Техническое обслуживание должно осуществляться только на основании обращения пользователя к заведующему отделом информатизации, а все обращения должны регистрироваться.

Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.

Дистанционное техническое обслуживание должно осуществляться только со специально выделенных автоматизированных рабочих мест, 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 конфиденциальной информации и временное изъятие носителей конфиденциальной информации (в том числе в составе АРМ) допускаются только с санкции пользователя. В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ.

Программное обеспечение должно устанавливаться со специальных сетевых ресурсов или съемных носителей, маркированных отделом информатизации, 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 информацию ограниченного доступа, должны быть закреплены за соответствующими сотрудниками Администрации. Запрещается использование указанных АРМ другими пользователями без согласования с заведующим отделом информатизации. При передаче указанного АРМ другому пользователю, должна производится гарантированная очистка диска (форматирование).

Заведующий отделом информатизации вправе отказать в устранении проблемы, вызванной наличием на рабочем месте программного обеспечения или оборудования, установленного или настроенного пользователем в обход действующей процедуры.

4.9. Порядок сопровождения ИС администрации Железнодорожного района города Барнаула

Обеспечение информационной безопасности информационных систем на стадиях жизненного цикла (ИБ ИС) должна обеспечиваться на всех стадиях жизненного цикла (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 заведующего отделом информатизации. Порядок разработки и внедрения ИС должен контролироваться заведующим отделом информатизации.

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 администратора информационной безопасности.

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 и (или) производства 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

модулей на весь срок их службы. В случае невозможности включения в договор (контракт) указанных требований к разработчику должна быть рассмотрена возможность приобретения полного комплекта рабочей документации на модуль, обеспечивающее возможность сопровождения ИС и их компонентов без участия разработчика. Если оба указанных варианта неприемлемы, например, вследствие высокой стоимости, руководство Администрации должно обеспечить анализ влияния угрозы невозможности сопровождения ИС и их компонентов на обеспечение непрерывности технологического процесса.

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 Администрации, и информации, используемой средствами обеспечения ИБ, из постоянной памяти или с внешних носителей.

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

4.9.1. Профилактика нарушений политик информационной безопасности

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

Проведение в ИС Администрации 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 Администрации степенью периодичности.

Задача предупреждения в ИС Администрации возможных нарушений информационной безопасности решается по мере наступления следующих событий:

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

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

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

Заведующий отделом информатизации (возможно, при помощи сторонней организации специализирующейся в области информационной безопасности) собирает и анализирует информацию о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения относительно ИС Администрации. Источниками подобного рода сведений могут служить официальные издания и публикации различных компаний, общественных объединений и других организаций, специализирующихся в области защиты информации.

Заведующий отделом информатизации (возможно, при помощи сторонней организации, специализирующейся в области информационной безопасности) организовывает периодическую проверку СЗИ ИС Администрации путем моделирования возможных попыток осуществления НСД к защищаемым информационным ресурсам.

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

Плановая разъяснительная работа по правилам настоящих политик, а также инструктаж сотрудников Администрации по соблюдению требований нормативных и регламентных документов по информационной безопасности, принятых в Администрации, проводится на усмотрение заведующего отделом информатизации.

Внеплановая разъяснительная работа по правилам настоящих политик, а также инструктаж сотрудников Администрации по соблюдению требований нормативных и регламентных документов по информационной безопасности, принятых в Администрации, 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.

4.9.2. Ликвидация последствий нарушения политик информационной безопасности

Заведующий отделом информатизации, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС Администрации, должен своевременно обнаруживать нарушения информационной безопасности, факты осуществления НСД к защищаемым информационным ресурсам и предпринимать меры по их локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения информационной безопасности или осуществления НСД к защищаемым информационным ресурсам ИС Администрации рекомендуется уведомить заведующего отделом информатизации, и далее следовать их указаниям.

Действия заведующего отделом информатизации при признаках нарушения политик информационной безопасности регламентируются следующими внутренними документами:

- Инструкцией пользователя автоматизированной системы;
- Политикой информационной безопасности;
- Должностными обязанностями заведующего отделом информатизации.

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

4.9.3. Ответственность нарушителей политик информационной безопасности

Ответственность за выполнение правил Политик безопасности несет каждый сотрудник Администрации в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования политики безопасности Администрации, 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 Администрации в результате нарушения ими правил политики ИБ (Ст. 238 Трудового кодекса РФ).

За умышленное причинение ущерба, а также за разглашение сведений, составляющих охраняемую законом тайну (служебную, коммерческую или иную), в случаях, предусмотренных федеральными законами, сотрудники Администрации несут материальную ответственность в полном размере причиненного ущерба (Ст. 243 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, уничтожение, блокирование или модификация защищаемой информации, сотрудники Администрации несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.

5. Регулирующие законодательные нормативные документы

При организации и обеспечении работ по информационной безопасности сотрудники Администрации должны руководствоваться следующими законодательными нормативными документами:

5.1. Основополагающие нормативные документы

К основополагающим нормативным документам относятся:

– Доктрина информационной безопасности Российской Федерации (утверждена Президентом РФ от 9 сентября 2000 г. № Пр-1895).

5.2. Законы Российской Федерации

– Закон Российской Федерации от 5 марта 1992 г. № 2446-I «О безопасности»;

– Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» (с изменениями от 8 ноября 2007 г.);

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

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

– Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» (с изменениями от 9 мая 2005 г., 1 мая, 1 декабря 2007 г.);

– Федеральный закон от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности» (с изменениями от 13, 21 марта, 9 декабря 2002 г., 10 января, 27 февраля, 11, 26 марта, 23 декабря 2003 г., 2 ноября 2004 г., 21 марта, 2 июля, 31 декабря 2005 г., 27 июля, 4, 29 декабря 2006 г., 5 февраля, 19 июля, 4, 8 ноября, 1, 6 декабря 2007 г.).

5.3. Указы и распоряжения президента Российской Федерации

– 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 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями от 23 сентября 2005 г.).

5.4. Постановления и распоряжения Правительства РФ

– 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»;

– Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации» (с изменениями от 23 апреля 1996 г., 29 марта 1999 г., 17 декабря 2004 г.);

– Постановление Правительства Российской Федерации от 17 ноября 2007 г. №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

5.5. Нормативные и руководящие документы Федеральных служб РФ

– Приказ ФСТЭК от 5 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»

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

– 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. 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 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);

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

– Постановление Главного государственного санитарного врача Российской Федерации от 3 июня 2003 г. № 118 «О введении в действие санитарно- эпидемиологических правил и нормативов СанПиН 2.2.2/2.4.1340-03» (с изменениями от 25 апреля 2007 г.).

5.6. 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 50922-96 «Защита информации. Основные термины и определения» (введен в действие постановлением Госстандарта России от 10 июля 1996 г. № 450);

– 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 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (введен в действие постановлением Госстандарта России от 12 мая 1999 г. № 160);

– 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).

Заведующий отделом информатизации М.А.Калинин

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 подразделения для создания пользовательской учетной записи в ИС Администрации	Включено в настоящий документ
2	Форма заявления на создание и изменение полномочий пользователю	Содержит форму заявления, оформляемого руководителем подразделения для наделения пользователя новыми полномочиями для работы с информационными ресурсами ИС Администрации	Включено в настоящий документ
3	Форма заявления на блокировку учетной записи пользователя	Содержит форму заявления, оформляемого руководителем подразделения для блокирования учетной записи пользователя	Включено в настоящий документ

Приложение 1
Форма заявления
на создание учетной
записи пользователя

СОГЛАСОВАНО
Главный специалист по кадрам «___» _____ 20__г.
(для штатных сотрудников)

Заведующий
отделом информатизации «___» _____ 20__г.

ЗАЯВЛЕНИЕ № _____
На создание (продление) учетной записи пользователя

Прошу создать (продлить) учетную запись пользователя:

Наименование органа администрации	
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.
(Ф.И.О. руководителя органа адм-ции) (подпись) (дата)

С правилами работы в информационной системе Администрации ознакомлен(а)

_____ _____ «___» _____ 20__г.
(Ф.И.О. сотрудника) (подпись) (дата)

Выполнено: _____ _____
(назначенное имя пользователя) (адрес корпоративной почты)

Системный администратор _____ _____ Системное Время: ____чч____мм
(Подпись) (Ф.И.О.)

Дата: «___» _____ 20__г.

Приложение 2
Форма заявления на
изменение полномочий

СОГЛАСОВАНО

Заведующий
отделом информатизации «___» _____ 20__г.

ЗАЯВЛЕНИЕ № _____
На изменение полномочий пользователю

Прошу изменить полномочия по работе с информационным ресурсом:

Наименование органа администрации	
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.
(Ф.И.О. руководителя органа адм-ции) (подпись) (дата)

С правилами работы в информационной системе Администрации и указанными службами ознакомлен

_____ _____ «___» _____ 20__г.
(Ф.И.О. сотрудника) (подпись) (дата)

Выполнено: _____
(назначенное имя пользователя, описание выполненных действий)

Системный администратор _____ _____ Системное Время: ____чч____мм
(Подпись) (Ф.И.О.)

Дата: «___» _____ 20__г.

Приложение 3
Форма заявления
на блокировку
учетной записи

СОГЛАСОВАНО
Главный специалист по кадрам «___» _____ 20__г.
(для штатных сотрудников)

Заведующий
отделом информатизации «___» _____ 20__г.

ЗАЯВЛЕНИЕ № _____
На блокировку учетной записи пользователя

Прошу заблокировать учетную запись пользователя:

Наименование органа администрации	
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.
(Ф.И.О. руководителя органа адм-ции) (подпись) (дата)

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

Пользователь блокирован

Системный администратор _____ _____ Системное Время: ____чч____мм
(Подпись) (Ф.И.О.)

Дата: «___» _____ 20__г.