

11

УТВЕРЖДАЮ  
Заместитель главы администрации,  
руководитель аппарата



О.В.Новикова

" 09 " 2024 г.

**ПОЛИТИКА  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ**

## **Вводные положения**

### **Введение**

Политика информационной безопасности Администрации Центрального 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.

### **Цели**

Основными целями политики ИБ являются защита информации Администрации и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в Положении.

Общее руководство обеспечением ИБ осуществляет заведующий отделом информатизации. Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет сотрудник, выполняющий функции администратора информационной безопасности (далее администратор информационной безопасности). Ответственность за функционирование автоматизированной системы учреждения несет заведующий отделом информатизации.

Должностные обязанности администратора информационной безопасности закрепляются в должностных инструкциях заведующего отделом информатизации.

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

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

### **Задачи**

Политика информационной безопасности 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, а именно:
  - Политика реализации антивирусной защиты;
  - Политика учетных записей;
  - Политика предоставления доступа к информационному ресурсу;
  - Политика использования паролей;
  - Политика защиты АРМ;
  - Политика конфиденциального делопроизводства;
- определение порядка сопровождения ИС Администрации.

### **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, а также в договорах.

### **Период действия и порядок внесения изменений**

Настоящая политика утверждается главой Администрации.

Политика признается утратившей силу главой Администрации.

Инициаторами внесения изменений в политику информационной безопасности являются:

- глава Администрации;
- заместитель главы Администрации, руководитель аппарата;
- заведующий отделом информатизации Администрации.

Плановая 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.

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

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

Ответственными за актуализацию политики информационной безопасности (плановую и внеплановую) несет администратор информационной безопасности.



Контроль за исполнением требований настоящей политики и поддержанием ее в актуальном состоянии возлагается на администратора информационной безопасности.

## 1. 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 учреждения, осуществляющих контроль за обеспечением защиты информации в локальной вычислительной сети (далее - ЛВС), а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления несанкционированного доступа (далее - 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 самостоятельно (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит). Результаты проверки документально оформляются в виде отчета об аудите.

*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.

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

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

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

*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 Администрации, привести к причинению Администрации материального или иного вида ущерба.

*Локальная вычислительная сеть (ЛВС)* – группа компьютеров, 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 сети, а также между сетью Администрации 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 (НСД)* – 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 взаимосвязанных 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



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 рабочей станции.

*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.

*Системный администратор* – 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.

*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, характеризующееся способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

*ЭВМ* – электронная - 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.

## **2. Обозначения и сокращения**

АРМ – Автоматизированное рабочее место.

АС – Автоматизированная система.

БД – База данных.

ЗИ – Защита информации.

ИБ – Информационная безопасность.

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.

## **3. Политики информационной безопасности Администрации. 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 Главой администрации.

### **Основные принципы обеспечения ИБ**

Основными принципами обеспечения ИБ являются следующие:

- Постоянный и всесторонний анализ информационного пространства Администрации с целью выявления уязвимостей информационных активов.
- Своевременное обнаружение проблем, потенциально способных повлиять на ИБ Администрации, 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 Администрации, а также повышать трудоемкость технологических процессов обработки информации.
- Контроль эффективности принимаемых защитных мер.
- Персонализация и адекватное разделение ролей и ответственности между сотрудниками Администрации, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

### **Соответствие политик безопасности действующему законодательству**

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

### **Ответственность за реализацию политик информационной безопасности**

Ответственность за разработку мер и контроль обеспечения защиты информации несёт администратор информационной безопасности.

Ответственность за реализацию политик возлагается:

- в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты – на администратора информационной безопасности;
- в части, касающейся доведения правил политик до сотрудников Администрации, а также иных лиц (см. область действия настоящей политики) – на администратора информационной безопасности;
- в части, касающейся исполнения правил политики, – на каждого сотрудника Администрации, согласно их должностным и функциональным обязанностям, попадающего под область действия настоящей политики.

### **Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе**

Организация повышения уровня сотрудников Администрации в области информационной безопасности возлагается на администратора информационной безопасности. Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по



информационной безопасности». Обучение сотрудников Администрации правилам работы с персональными данными, проводится путем:

- проведения администратором информационной безопасности инструктажа с сотрудниками, принимаемыми на работу в Администрации;
- самостоятельного изучения сотрудниками внутренних нормативных документов Администрации.

Допуск персонала к работе с защищаемыми информационными ресурсами Администрации осуществляется только после 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 персональными данными осуществляется после ознакомления с «Инструкцией по организации работы с материальными носителями персональных данных», «Инструкцией по организации работы с электронными носителями персональных данных».

### **Защищаемые информационные ресурсы Администрации**

Различаются следующие категории информационных ресурсов, подлежащих защите в Администрации:

*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 01.11.2012 г. № 1119 «Об утверждении Положения об обеспечении безопасности 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 Администрации, которую запрещено относить к конфиденциальной на основании законодательства России. Информация, представляемая в публичный доступ, используемая в хозяйственной деятельности Администрации;

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

Конфиденциальная информация представляет собой сведения ограниченного доступа, включая персональные данные, 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 определяются «Перечнем сведений конфиденциального характера в администрации Центрального района города Барнаула».

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 процессов Администрации.

Для этого в Администрации выполняются следующие мероприятия:

- определяется порядок работы с документами, содержащими персональные данные;
- устанавливается круг лиц и порядок доступа к подобной информации;
- вырабатываются меры по контролю обращения с документами, содержащими персональные данные;
- включаются в трудовые договоры с сотрудниками пункты о неразглашении конфиденциальных сведений и определяются санкции за нарушения порядка работы с ними и их разглашение.

Форма подписки о неразглашении сведений конфиденциального характера подписывается при заключении трудового договора, который подписывается всеми сотрудниками учреждения при приеме на работу в Администрацию. Защита конфиденциальной информации, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых Администрацией с другими организациями. Персональные данные сотрудника учреждения – 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 расписку;
- 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.

### **Организация системы управления информационной безопасностью Администрации**

Система управления информационной безопасности Администрации (СУИБ) – предназначенная 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 правовых рисков деятельности Администрации;
- 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 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.

### **Реализация системы управления информационной безопасностью**

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.

### **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 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 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 - 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.

### **Политика предоставления доступа к информационному ресурсу. Назначение**

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

#### **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, 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 Администрации одного и того же имени пользователя («группового имени») ЗАПРЕЩЕНО.



### **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 (Приложение № 1).

В заявке указывается:

- должность (с полным наименованием органа), фамилия, имя и отчество сотрудника;
- основание для регистрации учетной записи.

Заявку подписывает главный специалист по кадрам Администрации подтверждающий, что указанный сотрудник действительно принят в штат Администрации.

Заявка согласуется с администратором информационной безопасности и передается в отдел 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 ресурсам Администрации.

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

### **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).

Заявка согласуется и передается на исполнение администратору информационной безопасности.

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

### **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 главный специалист по кадрам 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 главный специалист по кадрам, утверждая тем самым факт прекращения срока действия полномочий пользователя.

Администратор информационной безопасности исполняет представленную заявку.

По окончании внесения изменений в заявку 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 администратором информационной безопасности, для исполнения требования по сохранению данных после выполнения действий по блокированию учетной записи.

### **Порядок хранения исполненных заявок**

Исполненные заявки передаются администратору информационной безопасности, и хранятся в архиве в течение 5 лет с момента окончания предоставления доступа к информационному ресурсу Администрации.

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 правильности настройки средств разграничения доступа к ресурсам системы.

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

### **Политика учетных записей. Назначение**

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

### **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 организации труда (например, посменное дежурство), использование общей учетной записи должно сопровождаться отметкой, 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.

#### **Политика использования паролей. Назначение**

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

#### **Положения политики**

Положения политики закрепляются в «Инструкции по организации парольной защиты».

#### **Политика реализации антивирусной защиты. Назначение**

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

#### **Положения политики**

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

#### **Политика защиты автоматизированных рабочих мест. Назначение**

Настоящая Политика определяет основные правила и требования по защите персональных данных и иной конфиденциальной информации Администрации от неавторизованного доступа, утраты или модификации.

#### **Положения политики**

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

При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие конфиденциальную информацию, 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, принятыми в Администрации, (согласно занимаемой должности), а именно с инструкциями по организации работы с материальными и электронными носителями персональных данных, 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 администратору информационной безопасности, а также сотрудникам отдела информатизации.

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 заведующему отделом информатизации и проводиться в соответствии с требованиями Инструкции по техническому обслуживанию.

Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.

Дистанционное техническое обслуживание запрещено.

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 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 конфиденциальную информацию, должны быть закреплены за соответствующими сотрудниками Администрации. Запрещается использование указанных АРМ другими пользователями без согласования с администратором информационной безопасности Администрации. При передаче указанного АРМ другому пользователю, должна производиться гарантированная очистка диска (форматирование).

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



## Порядок сопровождения ИС Администрации

Обеспечение информационной безопасности информационных систем должна обеспечиваться на всех стадиях жизненного цикла (ЖЦ) ИС, автоматизирующих технологические процессы, с учетом всех сторон, вовлеченных в процессы (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 администратора информационной безопасности. 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.xxx «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 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 Администрации, 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.

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 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.

### **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.

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 (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.

Администратор информационной безопасности (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.

Администратор информационной безопасности (возможно, при помощи сторонней организации, специализирующейся в области информационной безопасности) организывает 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, 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 администратором информационной безопасности один раз в полгода.

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.

### **Ликвидация последствий нарушения политик информационной безопасности**

Администратор информационной безопасности, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС, 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 рекомендуется уведомить администратора информационной безопасности и следовать его указаниям.

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

- Инструкцией по работе пользователя;
- Политикой информационной безопасности;
- Должностными обязанностями администратора информационной безопасности;

После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС.

#### **Ответственность нарушителей политики 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 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 Администрации несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.

#### **4. Регулирующие законодательные нормативные документы**

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

##### **Основополагающие нормативные документы**

К основополагающим нормативным документам относятся:

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

##### **Законы Российской Федерации**

- Закон Российской Федерации от 5 марта 1992 г. № 2446-1 «О безопасности»;
- Гражданский кодекс Российской Федерации;
- 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»;
- Уголовный кодекс РФ;
- 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.).

### **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 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.);

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

### **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»;

– 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.).

### **Нормативные и руководящие документы Федеральных служб РФ**

– 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 от 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 недеklarированных 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).

## **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 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).

## 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 Администрации	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 Администрации	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

Администратор  
информационной безопасности  
« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_  
(подпись)

Главный специалист по кадрам  
« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_  
(подпись)

## ЗАЯВЛЕНИЕ №

на создание (продление) учетной записи пользователя

Прошу создать (продлить) учетную запись пользователя:

Наименование органа администрации	
Ф.И.О. муниципального служащего, должность, телефон	
Ф.И.О. непосредственного руководителя, должность, телефон	

Муниципальный служащий приступает к работе с: « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г. по  
« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г. (указывается при необходимости)

Обоснование служебной  
необходимости: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
(Ф.И.О. руководителя органа администрации) (подпись)  
« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

С правилами работы в информационной системе администрации города ознакомлен(а)

\_\_\_\_\_  
(Ф.И.О. муниципального служащего)  
(подпись)

Выполнено: \_\_\_\_\_  
(назначенное имя пользователя) (адрес корпоративной почты)

Системный администратор: \_\_\_\_\_  
(Ф.И.О.) (Подпись)

Системное время: \_\_\_\_\_ чч \_\_\_\_\_ мм

Дата: « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

## Приложение 2. Форма заявления на изменение полномочий

СОГЛАСОВАНО

Администратор информационной безопасности

«\_\_» \_\_\_\_\_ 2010 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. начальник отдела) (подпись) (дата)

С правилами работы в информационной системе Администрации ознакомлен(на)

\_\_\_\_\_ «\_\_» \_\_\_\_\_ 20\_\_ г.  
(Фамилия И.О. сотрудника) (подпись) (дата)

Выполнено: \_\_\_\_\_  
(назначенное имя пользователя, описание выполненных действий)

Заведующий отделом информатизации \_\_\_\_\_ Системное  
(Подпись) (Фамилия И.О.)

Дата: «\_\_» \_\_\_\_\_ 20\_\_ г.



**Приложение 3. Форма заявления на блокировку учетной записи  
СОГЛАСОВАНО**

Администратор

информационной безопасности  
« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_ (подпись)

Главный специалист по кадрам  
« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_ (подпись)

**ЗАЯВЛЕНИЕ №**  
на блокировку учетной записи пользователя

Прошу заблокировать учетную запись пользователя:

Наименование органа администрации	
Ф.И.О. муниципального служащего, должность, телефон	
Имя в системе	
Ф.И.О. непосредственного руководителя, должность, телефон	

Срок действия полномочий прекратить с: « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Обоснование блокировки: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_ (Ф.И.О. руководителя органа администрации)

\_\_\_\_\_ (подпись)

С гарантированным хранением данных в течение \_\_\_\_\_  
(указывается срок хранения данных пользователя)

Системный администратор: \_\_\_\_\_ (Подпись) \_\_\_\_\_ (Ф.И.О.)

Системное время: \_\_\_\_\_ чч \_\_\_\_\_ мм

Дата: « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.