АДМИНИСТРАЦИЯ
ШАТРОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА
КУРГАНСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 13 января 2023 года № 08 с.Шатрово

Об утверждении политики информационной безопасности Администрации Шатровского муниципального округа Курганской области

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Стратегией развития информационного общества в Российской Федерации на 2017 — 2030 годы, утверждённой Указом Президента Российской Федерации от 9 мая 2017 года №203, Уставом Шатровского муниципального округа Курганской области, Администрация Шатровского муниципального округа Курганской области
ПОСТАНОВЛЯЕТ:

1. Утвердить политику информационной безопасности Администрации Шатровского муниципального округа Курганской области согласно приложению к настоящему постановлению.
2. Признать утратившим силу постановление Администрации Шатровского района от 9 июля 2018 года № 241 «Об утверждении политики информационной безопасности Администрации Шатровского района».
3. Обнародовать настоящее постановление в соответствии со ст. 44 Устава Шатровского муниципального округа Курганской области.
4. Контроль за выполнением настоящего постановления возложить на управляющего делами – руководителя аппарата Администрации Шатровского муниципального округа.

Глава Шатровского
муниципального округа
Курганской области Л.А.Рассохин

О.А.Ядрышникова
9 10 80
Разослано по списку (см. оборот)

Приложение
к постановлению Администрации
Шатровского муниципального округа
от 13 января 2023 года № 08
«Об утверждении политики информационной безопасности Администрации Шатровского муниципального округа Курганской области»

ПОЛИТИКА
информационной безопасности Администрации Шатровского муниципального округа Курганской области

Раздел I. Введение

Политика информационной безопасности (далее – Политика) Администрации Шатровского муниципального округа Курганской области (далее – Администрация) определяет цели и задачи системы обеспечения информационной безопасности (далее - ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Администрация в своей деятельности.

Основными целями политики ИБ являются защита информации Администрации Шатровского муниципального округа Курганской области и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в Уставе Шатровского муниципального округа Курганской области.

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 персонал Администрации. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне общества), 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.

Разработанная на основе прогноза политика ИБ и в соответствии с ней построенная система 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:

1) описание организации системы управления информационной безопасностью в Администрации;
2) определение основных направлений Политики информационной безопасности, а именно:

- Политика реализации антивирусной защиты;
- Политика учетных записей;

- Политика предоставления доступа к информационному ресурсу;
- Политика использования паролей;
- Политика защиты автоматизированного рабочего места;
- Политика конфиденциального делопроизводства;

3) определение порядка сопровождения информационных систем Администрации.

Раздел II. Область действия Политики

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

Общее руководство обеспечением ИБ осуществляет управляющий делами - руководитель аппарата Администрации Шатровского муниципального округа.

Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет сотрудник, отвечающий за функционирование автоматизированной системы и выполняющий функции администратора информационной безопасности (далее администратор информационной безопасности) в соответствии с инструкцией согласно Приложению 5 к настоящей Политике, и назначается распоряжением Главы Администрации.

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

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

Раздел III. Период действия и порядок внесения изменений

Настоящая Политика вводится в действие постановлением Администрации Шатровского муниципального округа Курганской области.

Инициаторами внесения изменений в политику информационной безопасности являются:

управляющий делами – руководитель аппарата Администрации Шатровского муниципального округа;

администратор информационной безопасности.

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

Внеплановая актуализация политики 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.

Контроль за выполнением требований настоящей политики и поддержанием ее в актуальном состоянии возлагается на управляющего делами – руководителя аппарата Администрации Шатровского муниципального округа.

Раздел IV. 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 Администрации, осуществляющий контроль за обеспечением защиты информации в ЛВС (локально вычислительная сеть), а также осуществляющий организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД (несанкционированный доступ к информации) к защищаемой информации.

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

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

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

Доступ к информации – возможность получения информации и ее использования.

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

Информационная безопасность – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов общества в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов общества.

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

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

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

Информационные средства – программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая

эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

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

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

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

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

Конфиденциальность – доступ к информации только авторизованных пользователей.

Критичная информация – информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование подразделений Администрации, привести к причинению Администрации материального или иного вида ущерба.

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 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 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 сети в установленном порядке и получивший права на доступ к ресурсам сети в соответствии со своими функциональными обязанностями.

Принятие риска – решение принять риск.

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

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

Регистрационная (учетная) запись пользователя – включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе Администрации 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.

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 Администрации (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер).

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

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

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.

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.

Раздел V. Назначение Политики информационной безопасности

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

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

Политика информационной безопасности относится к административным мерам обеспечения информационной безопасности и определяет стратегию Администрации в области ИБ.

Политика информационной безопасности регламентирует эффективную работу средств защиты информации. Она охватывает все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях. Политика информационной безопасности реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Все документально оформленные решения, формирующие Политику, должны быть утверждены Главой Шатровского муниципального округа Курганской области.

Раздел VI. Основные принципы обеспечения ИБ

Основными принципами обеспечения ИБ являются следующие:

1. Постоянный и всесторонний анализ информационного пространства общества с целью выявления уязвимостей информационных активов.
2. Своевременное обнаружение проблем, потенциально способных повлиять на ИБ общества, корректировка моделей угроз и нарушителя.
3. 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.
4. Контроль эффективности принимаемых защитных мер.
5. Персонификация и адекватное разделение ролей и ответственности между сотрудниками учреждения, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

Раздел VII. Соответствие ПБ 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, отраслевые и ведомственные документы, по вопросам безопасности информации различного уровня в пределах их компетенции.

Раздел VIII. Ответственность за реализацию Политики информационной безопасности

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

Ответственность за реализацию Политики возлагается:

в части, касающейся разработки и актуализации правил внешнего доступа, антивирусной защиты, а также доведения правил Политики до сотрудников Администрации – на администратора информационной безопасности;

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.

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

Организация просвещения 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 обращения с конфиденциальной информацией, проводится путем:

проведения администратором информационной безопасности инструктивных занятий с сотрудниками, принимаемыми на работу в Администрацию;

самостоятельного изучения сотрудниками внутренних нормативных документов Администрации.

Допуск персонала к работе с защищаемыми информационными ресурсами Администрации осуществляется только после его ознакомления с настоящей Политикой, а также после ознакомления пользователей с «Инструкцией пользователя ИС» в соответствии с приложением 9 к настоящей Политике, а также иными инструкциями в соответствии с приложениями 4,6,7,8,13 к настоящей Политике. Согласие на соблюдение правил и требований настоящей Политики подтверждается подписями сотрудников в «Журнале проведения инструктажа по информационной безопасности».

Допуск персонала к работе с конфиденциальной информацией Администрации осуществляется после ознакомления с «Инструкцией по учету материальных носителей конфиденциальной информации, регистрации их выдачи» в соответствии с приложением 12 к настоящей Политике. 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.

В отношении всех собственных информационных активов управления, активов, находящихся под контролем Администрации, а также активов, используемых для получения доступа к инфраструктуре управления, должна быть определена ответственность соответствующего сотрудника Администрации.

Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами Администрации должна доводиться до сведения управляющего делами – руководителя аппарата Администрации Шатровского муниципального округа.

Все работы в пределах Администрации должны выполняются в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в Администрации.

Внос в здание и помещения управления личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы Администрации производится только при согласовании с управляющим делами – руководителем аппарата Администрации Шатровского муниципального округа.

Все данные (конфиденциальные или строго конфиденциальные), составляющие тайну Администрации, хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы.

Руководители структурных подразделений должны периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам.

В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким.

Раздел X. 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 06.03.1997г. №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, 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 и порядок работы с конфиденциальными документами, определяются Инструкцией по учету материальных носителей конфиденциальной информации, регистрации их выдачи, в соответствии с Приложением 12 к настоящей Политике, а также «Перечнем сведений конфиденциального характера».

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, образцами изделиями и др., содержащими конфиденциальные сведения;
- устанавливается круг лиц и порядок доступа к подобной информации;
- вырабатываются меры по контролю обращения с документами, содержащими конфиденциальные сведения;
- включаются в трудовые договоры с сотрудниками обязательства о неразглашении конфиденциальных сведений и определяются санкции за нарушения порядка работы с ними и их разглашение.

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.

Раздел XI. Организация системы Управления информационной безопасностью Администрации

Организация системы Управления ИБ:

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 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.

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 Администрации 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, 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.

Политика предоставления доступа к информационному ресурсу.

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

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), также продления срока действия временной учетной записи пользователя для сотрудника Администрации инициируется заявкой в соответствии с приложением 1 к настоящей Политике.

В заявке указывается:

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

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

Заявка согласуется с управляющим делами – руководителем аппарата Администрации Шатровского муниципального округа и передается системному администратору (далее – системный администратор).

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

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

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

Порядок предоставления (изменения) полномочий пользователя:

процедура предоставления (или изменения) прав доступа пользователя к ресурсам Администрации инициируется заявкой сотрудника в соответствии с Приложением 2 к настоящей Политике.

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 с управляющим делами – руководителем аппарата Администрации Шатровского муниципального округа и передается системному администратору на исполнение.

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.

В заявке указывается:

- должность сотрудника, фамилия, имя и отчество сотрудника;
- имя пользователя (учетной записи) данного сотрудника;
- дата прекращения полномочий пользователя.

Управляющий делами - руководитель аппарата Администрации Шатровского муниципального округа рассматривает представленную заявку и передает заявку на исполнение системному администратору.

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

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

Такая заявка должна быть предварительно согласована с управляющим делами – руководителем аппарата Администрации Шатровского муниципального округа и после выполнения действий по блокированию учетной записи передается системному администратору для исполнения требования по сохранению данных.

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.

Копии исполненных заявок хранятся у системного администратора.

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 системным администратором правильности настройки средств разграничения доступа к ресурсам системы.

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

Политика учетных записей:

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

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

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

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

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

Политика использования паролей:

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

Положения политики закрепляются в «Инструкции по организации парольной защиты» в соответствии с Приложением 10 к настоящей Политике.

Политика реализации антивирусной защиты:

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

Положения политики закрепляются в «Инструкции по организации антивирусной защиты» в соответствии с Приложением 11 к настоящей Политике.

Политика защиты АРМ:

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

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

При любом оставлении рабочего места, АРМ должен быть заблокирован, 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 инструкциями по обращению с носителями конфиденциальной информации, «Перечнем сведений конфиденциального характера».

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

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

Пользователям запрещается устанавливать неавторизованные программы на компьютеры.

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

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

Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.

Дистанционное техническое обслуживание должно осуществляться только со специально выделенных 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 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.

Раздел XII. Порядок сопровождения ИС Администрации

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). Разработка технических заданий, проектирование, создание, тестирование, приемка средств и систем защиты ИС проводится при участии администратора информационной безопасности и системного администратора. Порядок разработки и внедрения ИС должен быть регламентирован и контролироваться.

При разработке ИС необходимо придерживаться требований и методических указаний, определенных стандартами, входящими в группу ГОСТ «Стандарты информационной технологии» и перечисленными в разделе 16 настоящей Политики.

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 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 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.

Раздел XIII. Профилактика нарушений Политики информационной безопасности

Под профилактикой нарушений Политики 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) осуществляет 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 Политики, а также инструктаж сотрудников Администрации по соблюдению требований нормативных и регламентных документов по информационной безопасности, принятых в Администрации, проводится администратором информационной безопасности ежеквартально.

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

проводится при пересмотре настоящей Политики, при возникновении инцидента нарушения правил настоящих политик.

Прием на работу новых сотрудников должен сопровождаться ознакомлением их с правилами и требованиями настоящей Политики.

Раздел XIV. Ликвидация последствий нарушения Политики 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 далее следовать его указаниям.

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

инструкцией пользователя ИС;

политикой информационной безопасности.

Должностными обязанностями администратора информационной безопасности.

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

Раздел XV. Ответственность нарушителей ПБ

Ответственность за выполнение правил Политики 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.

Управляющий делами – руководитель
Аппарата Администрации Шатровского
муниципального округа Т.И.Романова

Приложение 1
к Политике информационной безопасности
Администрации Шатровского
муниципального округа Курганской области

Форма заявки на создание учетной записи пользователя

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

Администратор информационной безопасности «___»
_____ 201 г.

ЗАЯВКА № _____
На создание (продление) учетной записи пользователя

Прошу создать (продлить) учетную запись пользователя:

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

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

Обоснование служебной необходимости:_____
_____
_____
____
_____ _____ «___» _____ 20__г.
(Ф. И.О.) (подпись) (дата)

С правилами работы в информационной системе Администрации ознакомлен(а)

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

Управляющий делами - руководитель аппарата
Администрации Шатровского района _____
(Подпись)

Дата: «___» _____ 201 г.

Приложение 2
к Политике информационной безопасности
Администрации Шатровского
муниципального округа Курганской области

Форма заявки на изменение полномочий

СОГЛАСОВАНО:

Администратор информационной безопасности «___» _____ 201 г.

ЗАЯВКА № _____
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:_____
_____
_____

С правилами работы в информационной системе Администрации ознакомлен(на)
_____ _____ «___» _____ 20__г.
(Фамилия И.О. сотрудника) (подпись) (дата)

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

Управляющий делами - руководитель аппарата
Администрации Шатровского муниципального округа _____
(Подпись)

Дата: «___» _____ 20__г.

Приложение 3
к Политике информационной безопасности
Администрации Шатровского
муниципального округа Курганской области

Форма заявки на блокировку учетной записи

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

Администратор информационной безопасности «___» _____ 201 г.

ЗАЯВКА № _____
На блокировку учетной записи пользователя

Прошу заблокировать учетную запись пользователя:

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

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

Обоснование
блокировки:_____
_____
_____
_____

_____ _____ «___»
_____ 20__г.
(Фамилия И.О. руководителя отдела) (подпись) (дата)

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

Пользователь блокирован

Управляющий делами - руководитель аппарата
Администрации Шатровского района _____
(Подпись)

Дата: «___» _____ 201 г.

Приложение 4
к Политике информационной безопасности
Администрации Шатровского
муниципального округа Курганской области

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных в Администрации Шатровского муниципального округа Курганской области

1. Общие положения.

Сотрудник, ответственный за обеспечение безопасности персональных данных в Администрации Шатровского муниципального округа Курганской области (далее – Администрация) назначается распоряжением Главы Администрации района из числа сотрудников Администрации.

Настоящая инструкция определяет функции, обязанности, права, ответственность сотрудника, ответственного за обеспечение безопасности персональных данных в Администрации.

2. Функции сотрудника, ответственного за обеспечение безопасности персональных данных в Администрации.

Контроль соблюдения сотрудниками, обрабатывающими персональные данные, правил обеспечения безопасности персональных данных.

Подготовка документов по защите персональных данных.

3. Обязанности сотрудника, ответственного за обеспечение безопасности персональных данных в Администрации.

Сотрудник, ответственный за обеспечение безопасности персональных данных в Администрации обязан:

обеспечивать выполнение режимных и организационных мероприятий на месте эксплуатации автоматизированных систем, а также следить за выполнением требований по условиям размещения средств вычислительной техники и их сохранность;

проводить инструктаж и консультации пользователей ПВЭМ по соблюдению режима конфиденциальности;

организовывать периодический контроль пользователей по соблюдению ими режима конфиденциальности, правил работы со съемными машинными носителями информации, выполнению организационных мер по защите информации, а также принимать участие в проведении проверок уполномоченными структурами;

взаимодействовать с администратором безопасности по вопросам обеспечения и выполнения требований обработки персональных данных;

организовывать работы по плановому контролю работоспособности технических средств защиты персональных данных, охраны объекта, средств защиты информации от несанкционированного доступа;

знать перечень установленных технических средств, входящих в состав информационных систем, и перечень задач, решаемых с их использованием;

контролировать целостность печатей (логотипов) на устройствах защищенных (допущенных к обработке персональных данных) компьютеров и серверов;

обеспечивать соблюдение сотрудниками утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств компьютеров и серверов из состава информационных систем;

хранить технические паспорта защищенных компьютеров и серверов, контролировать их соответствие реальным конфигурациям и вести учет изменений их аппаратно-программной конфигурации (заявки, на основании которых были произведены данные изменения);

осуществлять контроль за порядком учета, создания, хранения и использования резервных копий и машинных (выходных) документов, содержащих персональные данные;

контролировать порядок использования и обеспечения сохранности персональных устройств идентификации пользователей;

при выявлении возможных каналов неправомерного вмешательства в процесс функционирования информационных систем и осуществления несанкционированного доступа к персональным данным и техническим средствам из состава информационных систем, сообщать о них главе администрации;

инструктировать сотрудников по вопросам обеспечения информационной безопасности и правилам работы, с применяемыми средствами защиты информации.

4. Права сотрудника, ответственного за обеспечение безопасности персональных данных.

Сотрудник, ответственный за обеспечение безопасности персональных данных в Администрации, имеет право:

требовать от всех пользователей информационных систем персональных данных выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных;

участвовать в разработке мероприятий по совершенствованию безопасности персональных данных;

инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемых персональных данных и технических средств из состава информационных систем;

обращаться к руководителю с предложением о приостановке процесса обработки персональных данных или отстранению от работы пользователя в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности;

подавать свои предложения по совершенствованию организационных, технологических и технических мер защиты персональных данных.

5. Ответственность.

Сотрудник, ответственный за обеспечение безопасности персональных данных в Администрации, несет ответственность в соответствии с законодательством РФ за:

несоблюдение требований нормативных документов и инструкций, определяющих порядок обработки персональных данных;

разглашение персональных данных, ставших ему известными в связи с исполнением должностных обязанностей;

сохранность персональных данных.

Приложение 5
к Политике информационной безопасности
Администрации Шатровского
муниципального округа Курганской области

ИНСТРУКЦИЯ
администратора информационной безопасности в автоматизированных системах объектов информатизации Администрации Шатровского муниципального округа Курганской области

Общие положения.

Администратор информационной безопасности в автоматизированных системах объектов информатизации (далее – администратор информационной безопасности) в Администрации Шатровского муниципального округа Курганской области (далее – Администрация) назначается распоряжением Главы Администрации.

Настоящая инструкция определяет функции, обязанности, права, ответственность администратора информационной безопасности.

Функции администратора информационной безопасности:

1. Контроль за выполнением требований действующих нормативных документов по вопросам обеспечения режима конфиденциальности, при проведении работ в автоматизированных системах (АС) информационных систем персональных данных (ИСПДн) администрации (далее «АС ИСПДн»).

2.Настройка и сопровождение в процессе эксплуатации подсистемы управления доступом в «АС ИСПДн».

3. Контроль доступа лиц в помещение «АС ИСПДн».

4. Контроль за проведением периодической смены паролей для доступа пользователей в «АС ИСПДн».

5. Настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе в «АС ИСПДн».

6. Сопровождение подсистемы обеспечения целостности информации в «АС ИС- ПДн».

7. Анализ данных журналов аудита «АС ИСПДн» с целью выявления возможных нарушений требований защиты.

8. Оценка возможности и последствия внесения изменений в состав «АС ИСПДн» с учетом требований по защите, подготовка своих предложения.

9. Контроль физической сохранности средств и оборудования «АС ИСПДн».

10. Своевременный анализ журналов учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений.

11. В период профилактических работ на рабочих станциях «АС ИСПДн» снятие при необходимости средства защиты информации с эксплуатации с обязательным обеспечением сохранности информации.

12. Периодически предоставлять сотруднику, ответственному за обеспечение безопасности персональных данных отчет о состоянии защиты «АС ИСПДн» и о нештатных ситуациях и допущенных пользователями нарушений установленных требований по защи- те информации.

Обязанности администратора информационной безопасности:

- знать в совершенстве применяемые информационные технологии;
- знать права доступа пользователей по обработке, хранению и передаче защищаемой информации;
- обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах возложенных функций;
- проводить инструктаж пользователей по правилам работы в «АС ИСПДн»;

- в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

- докладывать сотруднику, ответственному за обеспечение безопасности персональных данных, о неправомерных действиях пользователя, приводящих к нарушению требований по защите информации;

- вести документацию в «АС ИСПДн» в соответствии с требованиями нормативных документов;

- настраивать только те параметры системы, которые определяют права доступа пользователей к информации;

- производить периодическое тестирование всех реализованных программно-техническими средствами функций и требований по обеспечению информационной безопасности;

- в соответствии с распоряжением управления и разрешительной системой доступа осуществлять добавление, блокирование, удаление и назначение прав доступа пользователям в системе;

- определить начальное значение паролей пользователя;

- восстанавливать настройки средств защиты информации при сбоях;

- хранить журналы аудита средств защиты информации на весь срок исковой давности действий и 5 лет после его окончания.

При выявлении факта несанкционированного доступа администратор информационной безопасности обязан:

- блокировать доступ к конфиденциальной информации;

- проанализировать характер несанкционированного доступа;

- доложить ответственному за обеспечение безопасности персональных данных служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях; -принять меры к защите от несанкционированного доступа;

- по решению ответственного за обеспечение безопасности персональных данных возобновить работу.

Права администратора информационной безопасности.

Администратор информационной безопасности в Администрации имеет право:

- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;

- требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

- блокировать учетные записи пользователей, осуществивших несанкционированный доступ к защищаемым ресурсам;

- участвовать в любых проверках в «АС ИСПДн»;

- запрещать устанавливать на серверах и рабочих станциях нештатное программное и аппаратное обеспечение; -вести контроль за процессом резервирования и дублирования важных ресурсов «АС ИСПДн»;

- участвовать в приемке новых программных средств;

- уточнять в установленном порядке обязанности пользователей «АС ИСПДн» по поддержанию уровня защиты;

- вносить предложения по совершенствованию уровня защиты «АС ИСПДн»;

- запрещать и немедленно блокировать попытки изменения программно-аппаратной среды «АС ИСПДн» без согласования порядка ввода новых (отремонтированных) технических и программных средств и средств защиты информации;

- запрещать и немедленно блокировать применение пользователям «АС ИСПДн» программ, с помощью которых возможны факты несанкционированного доступа к ресурсам «АС ИСПДн»;

- незамедлительно докладывать ответственному за обеспечение безопасности персональных данных обо всех попытках нарушения защиты «АС ИСПДн»;

- анализировать состояние защиты «АС ИСПДн» и ее отдельных подсистем;

- контролировать состояние средств и систем защиты информации и их параметры и критерии;

- контролировать правильность применения пользователями средств защиты информации;

- оказывать помощь пользователям в части применения средств защиты;

- не допускать установку, использование, хранение и размножение в «АС ИСПДн» программных средств, не связанных с выполнением функциональных задач;

- осуществлять контроль за соблюдением установленных правил и параметров регистрации и учета бумажных носителей информации;

- контролировать установленный порядок и правила антивирусной защиты информации;

- контролировать отсутствие на машинных носителях остаточной информации по окончании работы;

- не допускать к работе на рабочих станциях «АС ИСПДн» посторонних лиц.

Ответственность.

1. Ответственность за сохранность конфиденциальной информации несет администратор безопасности информации, действия которого фиксируются в протоколах аудита.

2. Администратор информационной безопасности несет ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования этих учетных записей.

3. При нарушениях администратором информационной безопасности правил, связанных с информационной безопасностью, он несет ответственность, установленную действующим законодательством Российской Федерации.

Приложение 6
к Политике информационной безопасности
Администрации Шатровского
муниципального округа Курганской области

ИНСТРУКЦИЯ
пользователя локальной вычислительной сети

1. Локальная вычислительная сеть (далее - ЛВС) Администрации Шатровского муниципального округа Курганской области (далее-Администрация) объединяет в единую информационную систему вычислительные ресурсы всех компьютеров использующихся в Администрации.

2. С целью оперативного обеспечения сотрудников управления вычислительными и информационными ресурсами регламентом работ определен круглосуточный режим работы ЛВС, включая выходные и праздничные дни.

3. Каждый сотрудник Администрации, допущенный к работе в информационной системе, является пользователем ЛВС. Все действия пользователей в ЛВС фиксируется многоуровневой системой аудита.

4. Пользователь получает от системного администратора индивидуальную учетную запись и соответствующий ему уникальный пароль доступа к ЛВС. Пароли входа в систему меняются системным администратором с определенной периодичностью, о чём предварительно оповещаются пользователи. Внеочередная смена пароля может произойти при потере информационного листа пароля, при переопределении прав доступа в сети в случае смены занимаемой должности (по ходатайству руководителя отдела) и при несанкционированном доступе, отраженном в журнале аудита, в целях отключения данного пользователя от сети до выяснения обстоятельств. Для внеочередной смены пароля следует обратиться к системному администратору. Если пользователь забыл свой пароль, необходимо получить его у администратора безопасности ЛВС. Пароль доступа в ЛВС является конфиденциальной информацией, дающей возможность получения закрытой информации из ЛВС и должен сохраняться пользователем в полном секрете от остальных пользователей. Знать пароль не имеет прав никто, кроме его владельца и системного администратора. В случае если в результате утечки информации постороннее лицо получит несанкционированный доступ к информации, сведения, о чём незамедлительно будут зафиксированы в протоколе сетевого аудита, полную ответственность за это будет нести владелец пароля, допустивший разглашения или утечку конфиденциальной информации. В случае непреднамеренного разглашения пароля пользователь обязан немедленно обратиться к системному администратору с целью блокировки пароля, его аннулирования и получения нового. Каждому паролю доступа к сети соответствует строго определенный список полномочий доступа владельца пароля к информации, ограниченные прав работы с информацией и пакетами прикладных программ. Изменение полномочий или расширение прав доступа пользователя к информации осуществляется по мотивированному письменному ходатайству руководителю отдела, в котором работает пользователь.

5. С целью предотвращения утечки информации каждый пользователь информационной системы управления обязан:

- не допускать прямого или косвенного разглашения пароля доступа к информационной системе управления;
- препятствовать попыткам посторонних лиц считать какую-либо информацию с экрана монитора;
- не оставлять посторонних лиц без присмотра в помещении, где установлена вычислительная техника;
- в случае длительного отсутствия в помещении предварительно выйти из пакета прикладных программ;

- принять меры к неразглашению за пределами управления сведений о специфике используемых пакетов прикладных программ, информационной системе, топологии сети и т.д.

Категорически запрещено считывание информации, копирование или запуск программ с носителей, посторонних лиц без предварительной проверки этой информации средствами антивирусной защиты.

6. С целью предотвращения отказов, сбоев и поломок оборудования каждый пользователь информационной системы Администрации при эксплуатации вычислительной техники обязан:

- не допускать попадания влаги на поверхность компьютера, принтера, монитора или клавиатуры;

- своевременно протирать экран монитора от загрязнения мягкой ветошью;

- соблюдать правила техники безопасности; с целью предотвращения падения оборудования следить за надёжной, устойчивой установкой на рабочем месте монитора и системного блока. В случае выхода оборудования из строя или нестабильной работы следует немедленно обратиться к руководителю отдела. В Администрации развернута система приема-передачи электронной почты. По всем вопросам эксплуатации электронной почты следует обращаться к системному администратору.

7. Пользователь ЛВС, совершивший действия, повлекшие нарушения работы информационной системы, несёт служебную, либо уголовную ответственность в соответствии со ст.ст. 272-274 Уголовного Кодекса Российской Федерации.

Приложение 7
к Политике информационной безопасности
Администрации Шатровского
муниципального округа Курганской области

ПОРЯДОК
использования (подключения) внешних USB – совместимых устройств

Внешние USB-накопители, используемые в Администрации Шатровского муниципального округа Курганской области должны быть идентифицированы и выданы под роспись пользователю информационной системы.

Запрещено подключение каких либо неучтенных USB-совместимых устройств к автоматизированным рабочим местам, на которых осуществляется обработка персональных данных, либо сведения составляющие, государственную тайну. Подключение съемных носителей следует производить при включенном компьютере и загруженной операционной системой. Если USB-накопитель в текущей сессии пользователя персонального компьютера будет использован только в «режиме чтения», то настоятельно рекомендуется, перед подключением USB-накопителя включить блокировку записи (если она предусмотрена конструкцией Вашего USB-устройства). Запрещено извлекать USB-накопитель из персонального компьютера в момент обращения к нему, это может привести к потере данных и повреждению устройства. Если при попытке извлечь USB-накопитель через значок "Безопасное извлечение устройства" появляется диалоговое окно "Проблема при извлечении "Запоминающее устройство для USB": Устройство Универсальный том не может быть остановлено прямо сейчас. Попробуйте остановить его позже", значит, открыты какие-то файлы с USB-накопителя. Закройте их и повторите попытку. Для сохранности и целостности данных не рекомендуется открывать файлы с данными со сменных носителей. Перед копированием файлов данных с внешних носителей настоятельно рекомендуется проверить носитель с помощью антивирусного сканера, установленного на персональном компьютере. Запрещается запускать или копировать с внешних носителей любые исполняемые файлы (приложения или командные файлы с расширениями exe, bat, com, cmd, inf, dll, scr) без согласования с администратором безопасности. Запрещено подключение к персональным компьютерам, находящимся в информационной системе Администрации USB совместимых устройств, таких как: переносные жесткие диски, цифровые фотоаппараты, телефоны и т.д. Подключение данных носителей возможно лишь под контролем администратора безопасности.

Приложение 8
к Политике информационной безопасности
Администрации Шатровского
муниципального округа Курганской области

ПОРЯДОК
резервного копирования информации

Резервное копирование информации автоматизированных систем Администрации Шатровского муниципального округа Курганской области (далее - Администрация) производится на основании следующих данных:

- состава и объема копируемых данных, необходимой периодичности проведения резервного копирования ;

- максимального срока хранения резервных копий -1 месяц;

- хранения 3-х следующих архивов: архив на 1-е число текущего месяца; архив среда-четверг, либо пятница-суббота текущей недели; архив сделанный в текущую ночь. Для снижения совокупной нагрузки на информационную систему все операции по резервированию информации необходимо проводить в не рабочее время (с 0 часов до 5 часов). Существуют три набора резервных копий: Месячный набор. Записывается информация на первое число текущего месяца. Срок хранения – месяц. Хранится на сервере резервного копирования. Недельная копия. Записывается в ночь на среду и в ночь на субботу. Срок хранения – субботняя копия – до следующей среды, вторничная копия – до субботы. Хранится на сервере резервного копирования. Ежедневная копия. Записывается ежесуточно, кроме ночи на среду и ночи на субботу. Срок хранения – сутки. Записывается на съёмный жёсткий диск. Съемный диск хранится в сейфе у администратора безопасности. На основе анализа данных автоматизированных систем администрации, возникает необходимость создания резервных копий следующей информации:

- информации, хранимой на файловом сервере Администрации;

- информации, хранимой непосредственно на персональных компьютерах в файловой системе - MS Windows. Базы данных информационных систем 1С «Бухгалтерия» и 1С «Зарплата + Кадры». Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации. Для организации системы резервного копирования в Администрации используется программное обеспечение «Мастер архивации и восстановления» (ntbackup.exe), которое является штатным средством резервного копирования для семейства операционных систем Microsoft Windows, а также обычное копирование данных на сервер резервного копирования. С целью оптимизации расходов на развёртывание системы резервного копирования, запись резервной копии осуществляется на жёсткий диск сервера резервного копирования. С помощью указанного программного обеспечения выполняются такие действия, как задание режимов и составление расписания резервного копирования клиентов, осуществляются операции по загрузке и выгрузке носителей информации, проводится контроль за состоянием выполнения заданий, запускаются процедуры восстановления информации. Резервное копирование баз данных информационных систем 1С «формации. Резервное копирование баз данных информационных систем 1С «Бухгалтерия» и 1С «Зарплата + Кадры» осуществляется средствами самой системы, с возможностью указания директории назначения на сервер резервного копирования администрации. При этом указывается срок хранения информации и периодичность выполнения резервного копирования. Любое восстановление информации, не вызванное необходимостью экстренного восстановления, связанной с потерей работоспособности информационной системы или ее компонентов, выполняется на основании заявки.

Приложение 9
к Политике информационной безопасности
Администрации Шатровского
муниципального округа Курганской области

ИНСТРУКЦИЯ
пользователю информационной системы

1. Общие обязанности сотрудников Администрации Шатровского муниципального округа по обеспечению информационной безопасности при работе с информационными системами.

Каждый оператор и сотрудник подразделений Администрации Шатровского муниципального округа участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным информационной системы (далее ИС), несет персональную ответственность за свои действия и обязан:

1) строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС;

2) знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (далее АРМ);

3) хранить в тайне свой пароль (пароли). В соответствии с «Инструкцией по организации парольной защиты» с установленной периодичностью менять свой пароль (пароли);

4) выполнять требования «Инструкции по организации антивирусной защиты» в части касающейся действий пользователей АРМ ИС;

5) немедленно вызывать ответственного за безопасность информации в подразделении и ставить в известность руководителя подразделения при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее НСД) к защищаемой АРМ;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на АРМ технических средств защиты;
- непредусмотренных формуляром АРМ отводов кабелей и подключенных устройств;

6) присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним АРМ в подразделении.

2. Сотрудникам Администрации Шатровского муниципального округа категорически запрещается:

1) использовать компоненты программного и аппаратного обеспечения ИС Администрации в неслужебных целях;

2) самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формулярами рабочих станций.

Приложение 10
к Политике информационной безопасности
Администрации Шатровского
муниципального округа Курганской области

ИНСТРУКЦИЯ
по организации парольной защиты

Данная инструкция призвана регламентировать организационно - техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе персональных данных (далее - ИСПД), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПД и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора информационной безопасности.

1. Правила формирования паролей.

1) личные пароли должны генерироваться и распределяться централизованно, либо выбираться пользователями информационной системы самостоятельно с учетом следующих требований: длина пароля должна быть не менее 6 символов;

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

3) пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abcd и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

4) при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях; личный пароль пользователь не имеет права сообщать никому.

В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников. При наличии технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение руководителю своего структурного подразделения. Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии у исполнителей), либо печать уполномоченного представителя отдела автоматизации (АСУ).

2. Ввод пароля.

При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерам и т.п.).

3. Порядок смены личных паролей.

Смена паролей должна проводиться регулярно, не реже одного раза в 3 месяца.

В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учётной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) администраторов информационной системы и других сотрудников, которым по роду работы были предоставлены полномочия системой парольной защиты.

Смена пароля производится самостоятельно каждым пользователем в соответствии с 1 настоящей инструкции, и/или в соответствии с указанием в системном баннере-предупреждении (при наличии технической возможности).

Временный пароль, заданный администратором информационной безопасности при регистрации нового пользователя, следует изменить при первом входе в систему.

4. Хранение пароля.

Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у администратора информационной безопасности, или руководителя подразделения.

5. Ответственность при организации парольной защиты.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

Приложение 11
к Политике информационной безопасности
Администрации Шатровского
муниципального округа Курганской области

ИНСТРУКЦИЯ
по организации антивирусной защиты

1. Настоящая инструкция определяет требования к организации защиты информационной системы (далее ИС) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее вредоносное ПО), устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих ИС Администрации Шатровского муниципального округа за их выполнение.

2. К использованию в Администрации Шатровского муниципального округа допускаются только лицензионные антивирусные средства, централизованно закупленные администратором у разработчиков (поставщиков) указанных средств. Установка средств антивирусного контроля на компьютерах осуществляется уполномоченным сотрудником, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

3. Применение средств антивирусного контроля.

Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС - при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов автоматизированных рабочих мест (далее АРМ).

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед архивированием, отправкой или записью на съемный носитель.

Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вредоносного ПО. Непосредственно после установки (изменения) программного обеспечения должна быть выполнена антивирусная проверка.

Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале подразделения за подписью лица, установившего (изменившего) программное обеспечение, и лица, его контролировавшего. При возникновении подозрения на наличие вредоносного ПО (ошибки в работе программ, появление графических и звуковых эффектов, искажения данных, пропадание файлов, частое появление сообщений о системных ошибках, замедление работы компьютера и т.п.) сотрудник структурного подразделения самостоятельно или вместе с ответственным за обеспечение безопасности информации должен провести внеочередной антивирусный контроль своего АРМ. ПО.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники Администрации обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и ответственного за обеспечение информационной безопасности, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов).

4. Ответственность.

Ответственность за организацию антивирусного контроля в структурном подразделении Администрации, эксплуатирующем ИС в соответствии с требованиями настоящей Инструкции, возлагается на руководителя.

Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение безопасности информации и всех сотрудников подразделения, являющихся пользователями ИС.

Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а также проверка работоспособности программы), а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками структурных подразделений Администрации осуществляется главным специалистом организационного отдела аппарата Администрации Шатровского муниципального округа.

Приложение 12
к Политике информационной безопасности
Администрации Шатровского
муниципального округа Курганской области

ИНСТРУКЦИЯ
по учету материальных носителей конфиденциальной информации, регистрации их выдачи

1. Настоящее инструкция регламентирует порядок учета, хранения и регистрации выдачи материальных носителей конфиденциальной информации.

2. Под материальными носителями информации в настоящей инструкции понимаются следующие носители информации:

- бумажные документы;
- магнитные, магнито-оптические диски;
- оптические диски (CD, DVD), в том числе, однократной и многократной записи;
- электронные накопители информации (флэш-память, жесткие диски).

3. Порядок хранения и учета материальных носителей.

Материальные информационные носители, содержащие конфиденциальную информацию, подлежат обязательному учету.

Носители должны храниться в сейфе, расположенном в помещении Администрации, и изыматься только для работы.

При поступлении материального информационного носителя, содержащего конфиденциальную информацию, администратор информационной безопасности регистрирует его в журнале учета материальных носителей.

Материальные носители, которые не являются необходимыми для выполнения постоянных служебных обязанностей, хранятся в отдельно отведенном сейфе не более 1 года, после чего их необходимо уничтожить с последующей регистрацией в журнале учета уничтоженных материальных носителей

4. Порядок регистрации выдачи материальных носителей.

Для учета выданных возвращенных материальных носителей необходимо вести журнал регистрации выдачи материальных носителей, в котором указываются дата, время, фамилия, имя и отчество должностного лица, получившего материальный носитель, роспись.

В случае возврата должностным лицом материального носителя в журнале регистрации выдачи материальных носителей проставляется отметка о возврате с указанием даты, времени возврата, личных подписей передающей и принимающей стороны.

5. Ответственность.

Персональную ответственность за соблюдение требований настоящей инструкции несут руководители отделов Администрации Шатровского муниципального округа.

Разглашение конфиденциальной информации и нарушение порядка обращения с документами, содержащими такую информацию, должностные лица, имеющие допуск к указанным сведениям, могут быть привлечены к дисциплинарной или иной предусмотренной законодательством Российской Федерации ответственности.

Приложение 13
к Политике информационной безопасности
Администрации Шатровского
муниципального округа Курганской области

ИНСТРУКЦИЯ
по физической охране ИСПД, контролю доступа в помещение

1. Настоящая Инструкция регламентирует условия и порядок осуществления доступа лиц в помещения со средствами информационной системы (далее ИС), обрабатывающими конфиденциальную информацию в целях обеспечения предотвращения несанкционированного доступа к персональным данным (далее ПД).

2. При обеспечении доступа лиц соблюдаются требования по защите ПД.

3. Обеспечение доступа лиц в помещения предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности подразделений и определяет порядок пропуска сотрудников подразделений, сотрудников иных учреждения и граждан в помещение.

4. Контроль за порядком обеспечения доступа лиц в помещения возлагается на руководителя структурного подразделения Администрации.

5. Помещения и оборудование размещены таким образом, чтобы исключить возможность бесконтрольного проникновения в эти помещения и к этому оборудованию посторонних лиц.

6. Не допускается нахождение сотрудников Администрации в помещениях Администрации во внерабочее время без особого распоряжения.

Основанием нахождения сотрудника во внерабочее время в помещении является «Перечень лиц, имеющим допуск в помещение».

В помещение пропускаются:

беспрепятственно:

руководители вышестоящих структурных подразделений;

сотрудники, имеющие допуск к работе с конфиденциальной информацией и с целью выполнения функциональных обязанностей;

при наличии служебного удостоверения:

сотрудники контролирующих органов;

сотрудники пожарных и аварийных служб, сотрудники полиции;

ограниченно:

сотрудники сторонних организаций для выполнения договорных отношений.

Посетители пропускаются в административное здание в рабочее время.

В помещениях, где происходит обработка и хранение ПД запрещено фотографирование, видеозапись, звукозапись, а также использование мобильных телефонов.

7. Организация и порядок производства ремонтно-строительных работ в здании Администрации.

Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных руководством.

Для предотвращения несанкционированного доступа к информации, содержащей ПД, следует контролировать деятельность рабочих.

8. Организация охраны.

Для исключения несанкционированного доступа к информации, содержащей ПД, при покидании помещения необходимо запирать его на ключ.

9. Уборка помещений.

Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.

Во время уборки в помещении должна быть приостановлена работа с ПД, должны быть выключены все ЭВМ, на которых хранятся ПД, носители, содержащие ПД должны быть убраны в сейф.

10. Требования по техническому укреплению.

Руководители структурных подразделений Администрации обеспечивают обязательное выполнение мероприятий по техническому укреплению и оборудованию специальными техническими средствами охраны, системами пожарной безопасности и должны руководствоваться следующими основными требованиями: двери и окна должны иметь прочные и надежные петли, шпингалеты, крючки или задвижки и быть плотно подогнаны к рамам и дверным коробам. Допускается применение электромеханических, электромагнитных замков и задвижек.