Российская Федерация
Тверская область

АДМИНИСТРАЦИЯ ЗУБЦОВСКОГО РАЙОНА

РАСПОРЯЖЕНИЕ
г. Зубцов

19.03.2019 № 46-р

О политике информационной безопасности
Администрации Зубцовского района

Во исполнение Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в целях обеспечения информационной безопасности в Администрации Зубцовского района

1 .Утвердить политику информационной безопасности Администрации Зубцовского района (прилагается).

2 . Заведующей общим отделом Администрации Зубцовского района В.Ю. Аракасовой ознакомить под подпись муниципальных служащих и служащих Администрации Зубцовского района с настоящим распоряжением.

3. Контроль за исполнением настоящего распоряжения оставляю за собой.

4. Настоящее распоряжение вступает в силу со дня его подписания.

Глава Зубцовского района Е.А. Николаева

Приложение к распоряжению
Администрации Зубцовского района

Политика информационной безопасности
Администрации Зубцовского района

1. Общие положения

1.1. Политика информационной безопасности Администрации Зубцовского района (далее - Политика) определяет цели и задачи системы обеспечения информационной безопасности (далее - ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Администрация Зубцовского района в своей деятельности.

1.2. Основными целями Политики Администрации Зубцовского района являются защита информации, организация и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении полномочий по решению вопросов местного значения и полномочий по осуществлению отдельных государственных полномочий, переданных органам местного самоуправления.

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

Наибольшими потенциальными возможностями для нанесения ущерба Администрации Зубцовского района располагают ее муниципальные служащие (далее - служащие). Действия служащих могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне Администрации Зубцовского района) либо иметь непреднамеренный ошибочный характер. Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией служащих и их способностью к адекватным действиям в нештатной ситуации.

Для противодействия угрозам ИБ в Администрации Зубцовского района на основе имеющегося опыта составляется прогностическая модель предполагаемых угроз и модель нарушителя.

Разработанная на основе прогноза Политика и в соответствии с ней построенная система управления РЕБ (далее — СУИБ) является наиболее правильным и эффективным способом минимизации рисков нарушения ИБ для Администрации Зубцовского района. 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 служащих .

1.4. Задачами политики являются:

описание организации системы управления информационной безопасностью в Администрации Зубцовского района;

определение структуры Политики ИБ Администрации Зубцовского района как следующих составных частей:

система мероприятий по реализации антивирусной защиты;

система мероприятий по ведению учетных записей;

система мероприятий по предоставлению доступа к информационному ресурсу;

система мероприятий по использованию информационного ресурса в рамках существующих информационных систем;

система мероприятий по использованию паролей;

система мероприятий по защите автоматизированных рабочих мест (далее - АРМ);

система мероприятий работы с носителями информации ограниченного доступа; определение порядка сопровождения информационных систем (далее - ИС) Администрации Зубцовского района.

1.5. Область действия Политики распространяется на все структурные подразделения Администрации Зубцовского района и обязательна для исполнения всеми служащими. Положения настоящей Политики применимы для использования в правовых актах Администрации Зубцовского района, а также в договорах и иных документах.

1.6. Политика вводится в действие и признается утратившей силу постановлением Администрации Зубцовского района.

Изменения в Политику вносятся распоряжением Администрации Зубцовского района. Инициатором внесения изменений в Политику является главный специалист, администратор Администрации Зубцовского района.

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

Внеплановая актуализация Политики производится в обязательном порядке в следующих случаях: при изменении политики Российской Федерации в области ИБ, правовых актов в области защиты информации; при изменении нормативных Документов (инструкций, положений, руководств), касающихся ИБ Администрации Зубцовского района; при происшествии и выявлении нарушений ИБ, могущих причинить ущерб Администрации Зубцовского района.

2. Термины и определения

Автоматизированная система - система, состоящая из служащих Администрации Зубцовского района и комплекса средств автоматизации ее деятельности, реализующая информационную технологию выполнения установленных функций.

Администратор ИБ - служащий или группа служащих Администрации Зубцовского района, осуществляющих контроль за обеспечением защиты информации в локальной вычислительной сети, а также осуществляющих организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления несанкционированного доступа к защищаемой информации.

Администратор сети - служащий или группа служащих Администрации Зубцовского района, осуществляющих непосредственную организацию и выполнение работ по созданию (модернизации), техническому обслуживанию и управлению (администрированию) информационной управляющей локальной вычислительной сети (далее - ЛВС), включая технические аспекты ИБ.

Актив - информация, представляющая ценность для Администрации Зубцовского района.

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

Аудит ИБ - процесс проверки выполнения установленных требований по обеспечению ИБ. Может проводиться как самой организацией (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит). Результаты проверки документально оформляются свидетельством аудита.

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

Владелец информационных активов - служащий Администрации Зубцовского района, получивший на основании соответствующего распоряжения права обладателя информации, обрабатываемой в информационной системе.

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

Доступ к информации - возможность получения информации и ее использования.

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

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

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

Идентификатор доступа - уникальный признак субъекта или объекта доступа.

Идентификация - присвоение субъектам доступа (пользователям, процессам) * 4 и объектам доступа (информационным ресурсам, устройствам) идентификатора и ^ (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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

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

Информационная среда - совокупность информационнотелекоммуникационной системы Администрации Зубцовского района, процессов, источников и потребителей информации, обслуживающего служащих и пользователей информационных систем, обеспечивающая автоматизацию производственных процессов Администрации Зубцовского района.

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

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

Информационные ресурсы - совокупность содержащейся в базе данных (далее БД) информации и обеспечивающих ее обработку информационных технологий, используемая в рабочих процессах Администрации Зубцовского района.

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

Информация - актив, который, подобно другим активам Администрации Зубцовского района, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Инфраструктура открытых ключей - технологическая инфраструктура и сервисы, обеспечивающие безопасность информационных и коммуникационных систем на основе использования криптографических алгоритмов и сертификатов ключей подписей.

Инцидент ИБ - действительное, предпринимаемое или вероятное нарушение ИБ, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов Администрации Зубцовского района.

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

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

Конфиденциальность - доступ к информации только санкционированных пользователей.

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

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

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

Локальная вычислительная сеть - группа персональных компьютеров (далее - ПК), а также периферийное оборудование, объединенные одним или несколькими

геномными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

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

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

Мониторинг ИБ - постоянное наблюдение за объектами, влияющими на обеспечение ИБ, сбор, анализ и обобщение результатов наблюдения под заданные цели. Объектом мониторинга в зависимости от целей может быть АС или ее часть, информационные технологические процессы Администрации Зубцовского района, информационные услуги Администрации Зубцовского района и пр.

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

Обработка риска - процесс выбора и осуществления мер по модификации

Операционная система (далее - ОС) - системная программа, осуществляющая взаимодействие пользователя и прикладных программ с аппаратной частью ПК.

Отдел Администрации Зубцовского района - структурное подразделение Администрации Зубцовского района с самостоятельными функциями, задачами и ответственностью, закрепленными в Положении о нем.

Остаточный риск - риск, остающийся после обработки риска.

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

Оценка риска — общий процесс анализа риска и оценивания риска.

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

Периметральное средство защиты информации (далее - СЗИ) - шлюз информационной безопасности, обеспечивающий межсетевое экранирование и защиту данных, пересылаемых по открытым каналам связи (шифрование), а также фильтрацию вредоносного программного обеспечения (далее - ПО) и блокирование внешних атак.

Политика ИБ - комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в учреждении для обеспечения его ИБ.

Пользователь ЛВС - служащий Администрации Зубцовского района (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированные в корпоративной сети в

устанвленном порядке и получившие права на доступ к ресурсам корпоративной сети в соответствии со своими функциональными обязанностями.

Принятие риска - решение принять риск.

Программное обеспечение — совокупность системных и прикладных программ, установленных на сервере или персональном компьютере.

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

Регистрационная (учетная) запись пользователя - запись, которая включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в ОС (сети, БД, приложении и т.п.), регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления БД, в сетевых доменах, «приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название органа Администрации, телефоны, адрес его электронной почты и т.п.

Роль - совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных

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

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

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

Системный администратор - служащий Администрации Зубцовского района, занимающийся сопровождением АС, отвечающий за функционирование локальной сети Администрации Зубцовского района и персональных компьютеров.

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

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

Средства криптографической защиты информации - средства шифрования, средства имитозащиты, средства электронной подписи, средства кодирования,средства изготовления ключевых документов (независимо от вида носителя речевой информации), ключевые документы (независимо от вида носителя речевой 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 ИБ в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер).

Уязвимость - недостатки или слабые места информационных активов, которые могут привести к нарушению ИБ Администрации Зубцовского района при реализации угроз в информационной сфере.

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

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

VPN (Virtual Private Network) - «виртуальная частная сеть»: технология и организация систематической удаленной связи между выбранными группами узлов в крупных распределенных сетях.

3. Обозначения и сокращения

АРМ - автоматизированное рабочее место
АС - автоматизированная система
БД - база данных
ИБ - информационная безопасность

ИОК - инфраструктура открытых ключей

ИС - информационная система

НСД - несанкционированный доступ

ОС - операционная система

ПО - программное обеспечение

СЗИ - средство защиты информации

СУИБ - система управления информационной безопасностью

ПК - персональный компьютер

4. Системы мероприятий ИБ Администрации Зубцовского района

4.1. Назначение систем мероприятий ИБ

Системы мероприятий ИБ Администрации Зубцовского района - это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в Администрации Зубцовского района.

Под системами мероприятий ИБ понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Системы мероприятий ИБ относятся к административным мерам ее обеспечения и определяют стратегию Администрации Зубцовского района в области ИБ.

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

Все документально оформленные решения, формирующие системы мероприятий, должны быть утверждены Главой Зубцовского района.

4.2. Основные принципы обеспечения ИБ

Основными принципами обеспечения ИБ являются следующие:

4.2.1. Постоянный и всесторонний анализ информационного пространства Администрации Зубцовского района с целью выявления уязвимостей информационных активов;

4.2.2. Своевременное обнаружение проблем, потенциально способных повлиять на ИБ Администрации Зубцовского района, корректировка моделей угроз и нарушителя;

4.2.3. 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 Администрации Зубцовского района, а также повышать трудоемкость [й] дологических процессов обработки информации;

4.2.4. Контроль эффективности принимаемых защитных мер;

4.2.5. Персонификация и адекватное разделение ролей и ответственности между служащими Администрации Зубцовского района, исходя из принципа персональной ответственности за совершаемые операции.

4.3. Соответствие систем мероприятий действующему законодательству.

Правовую основу систем мероприятий составляют федеральные законы и другие законодательные акты, определяющие права и ответственность граждан, органов государственной власти и органов местного самоуправления в сфере безопасности, а также нормативные, отраслевые и ведомственные документы по вопросам безопасности информации, утвержденные органами исполнительной власти Российской Федерации и Тверской области в пределах их компетенции.

4.4. Ответственность за реализацию систем мероприятий ИБ

Ответственность за реализацию систем мероприятий возлагается: в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты - на системного администратора; в части, касающейся исполнения правил систем мероприятий, - на каждого муниципального служащего Администрации Зубцовского района, согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей Политики.

4.5. Порядок подготовки служащих по вопросам ИБ и допуска их к работе

Организация обучения служащих Администрации Зубцовского района в области ИБ возлагается на главного специалиста, системного администратора. Подписи служащих об ознакомлении заносятся в Журнал проведения инструктажа по ИБ (Приложение 1). Обучение служащих Администрации Зубцовского района правилам обращения с информацией ограниченного доступа проводится путем: проведения системным администратором инструктивных занятий с служащими, принимаемыми на работу в администрацию Зубцовского района; самостоятельного изучения муниципальным служащим документов, реализующих Политику ИБ Администрации Зубцовского района.

Допуск служащих к работе с информационными ресурсами Администрации Зубцовского района осуществляется только после их ознакомления с системами мероприятий ИБ, а также после ознакомления пользователей с Инструкцией по работе пользователей в АС Администрации Зубцовского района, а также иными инструкциями пользователей отдельных ИС. Согласие на соблюдение правил и требований систем мероприятий ИБ подтверждается подписями служащих в Журнале проведения инструктажа по ИБ.

Допуск служащих к работе с информацией ограниченного доступа Администрации Зубцовского района осуществляется послё ознакомления с Инструкциями по обращению с носителями информации ограниченного

распространеиия. Правила допуска к работе с информационными ресурсами лиц, не являющихся служащими Администрации Зубцовского района, определяются на договорной основе с лицами или с организациями, представителями которых эти лица являются.

4.6. Защищаемые информационные ресурсы Администрации Зубцовского района.

Различаются следующие категории информационных ресурсов, подлежащих защите в Администрации Зубцовского района:

Информация ограниченного доступа (конфиденциальная) - информация, определенная в соответствии с федеральными законами от 27.07.2006 № 149-ФЗ ((0б информации, информационных технологиях и о защите информации», от 27,07.2006 № 152-ФЗ «О персональных данных», Указом Президента Российской федерации от 06.03.1997 № 188 «Об утверждении перечня сведений £ конфиденциального характера», Постановлением Правительства Российской '7 федерации от 17.11.2007 №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», предусмотренная Перечнем сведений конфиденциального характера.

Публичная информация - информация, получаемая из публичных источников (публикации в средствах массовой информации, теле- и радиовещание и т.д.), а также информация, предназначенная для размещения на внешних публичных ресурсах.

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

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

Подходы к решению проблемы защиты информации в Администрации Зубцовского района состоят в исключении неправомерных или неосторожных Действий со сведениями, относящимися к информации ограниченного распространения, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования рабочих процессов Администрации Зубцовского района.

Для этого в Администрации Зубцовского района выполняются следующие мероприятия: определяется порядок работы с документами, носителями и др.,

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

Подписка о неразглашении конфиденциальной информации совершается при

заключении трудового договора, который подписывается каждым муниципальным служащим при приеме на работу в администрацию Зубцовского района. Защита информации ограниченного доступа, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых администрацией Зубцовского района с другими организациями.

4.7. Организация СУИБ Администрации Зубцовского района

СУИБ Администрации Зубцовского района предназначена для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения ИБ Администрации Зубцовского района.

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

4.8. Реализация СУИБ Администрации Зубцовского района

В СУИБ реализуются 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 набор подходов к управлению рисками в ИБ, методология управления ими, 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 Зубцовского района 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, оцтролируютсл изменения факторов риска (активов, угроз, уязвимостей), сводятся аудиты и выполняются различные контролирующие процедуры.

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

4.9. Методы оценивания информационных рисков

Оценка информационных рисков Администрации Зубцовского района выполняется по следующим основным этапам: идентификация и количественная оценка информационных ресурсов, значимых для работы Администрации Зубцовского района; оценивание возможных угроз; оценивание существующих уязвимостей; оценивание эффективности средств обеспечения ИБ.

Предполагается, что значимые для производственного процесса уязвимые информационные ресурсы Администрации Зубцовского района 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 ИБ.

Цель оценивания рисков состоит в определении характеристик рисков корпоративной информационной системы и ее ресурсов. В результате оценки рисков становится возможным выбрать средства, обеспечивающие желаемый уровень ИБ Администрации Зубцовского района.

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 Зубцовского района.

При этом вероятность того, что угроза реализуется, определяется следующими основными показателями: привлекательностью ресурса, показатель используется при рассмотрении угрозы от умышленного воздействия со стороны человека; возможностью использования ресурса для получения дохода, показатель используется при рассмотрении угрозы от умышленного воздействия со стороны человека; техническими возможностями реализации угрозы, показатель используется при умышленном воздействии со стороны человека; степенью легкости, с которой уязвимость может быть использована.

4.10. Порядок предоставления доступа к информационному ресурсу

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

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

В случае производственной необходимости некоторым муниципальным служащим могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими служащими при работе в Администрации Зубцовского района одного и того же имени пользователя («группового имени») запрещается.

4.11. Порядок создания (продления) учетной записи пользователя

Процедура регистрации (создания учетной записи), также продления срока Г действия временной учетной записи пользователя для муниципального служащего Администрации Зубцовского района инициируется распоряжением Главы Зубцовского района.

Системный администратор совершает необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля и минимальных прав доступа к сетевым ресурсам Администрации Зубцовского района, таких, как право регистрации на АРМ муниципального служащего и пользования корпоративной электронной почтой.

4.12. Порядок предоставления (изменения) полномочий пользователя

Процедура предоставления (или изменения) прав доступа пользователя к ресурсам Администрации Зубцовского района инициируется распоряжением Администрации Зубцовского района.

4.13. Порядок удаления учетной записи пользователя

При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение муниципального служащего) учетная запись должна немедленно блокироваться. При этом системный администратор Администрации Зубцовского района должен быть уведомлен.

Системный администратор производит блокировку учетной записи пользователя.

4.14. Система мероприятий ведения учетных записей

Настоящая система мероприятий ИБ определяет основные правила присвоения учетных записей пользователям информационных активов Администрации Зубцовского района.

Регистрационные учетные записи подразделяются на: пользовательские, предназначенные для идентификации/аутентификации пользователей информационных активов Администрации Зубцовского района; системные, используемые для нужд ОС; служебные, предназначенные для обеспечения функционирования отдельных процессов или приложений.

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

Запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или Администрации Зубцовского района труда (например, посменное дежурство), использование общей учетной записи должно сопровождаться отметкой в журнале событий ОС, 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 ОС и должны использоваться только в случаях, предписанных документацией на ОС.

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

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

4.15.Система мероприятий по использованию паролей

Настоящая система мероприятий определяет основные правила обращения с паролями, используемыми для доступа к информационным активам Администрации Зубцовского района. Положения системы мероприятий закрепляются в Инструкции по организации парольной защиты в АС.

4.16.Система мероприятий реализации антивирусной защиты

Настоящая система мероприятий определяет основные правила для реализации антивирусной защиты в Администрации Зубцовского района.

Положения системы мероприятий закрепляются в Инструкции по проведению антивирусного контроля в АС.

4.17. Система мероприятий защиты АРМ

4.17.1. Настоящая система мероприятий определяет основные правила и требования по защите информации ограниченного доступа Администрации Зубцовского района от неавторизованного доступа, утраты или модификации.

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

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

4.17.4. 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;

4.17.5. Служащие получают доступ к ресурсам вычислительной сети после ознакомления с документами, регулирующими защиту персональных данных и утвержденными администрацией Зубцовского района согласно занимаемой должности;

4.17.6. Доступ к компонентам ОС и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставлено только системному администратору. Конечным пользователям предоставляется доступ только к тем командам, которые неообходимы для выполнения их должностных обязанностей;

4.17.7. Доступ к корпоративной информации предоставляется только лицам, рдеющим обоснованную необходимость в работе с этими данными для исполнения своих должностных обязанностей;

4.17.8. Пользователям запрещается устанавливать ПО на компьютеры без согласования с системным администратором;

4.17.9. Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неразрешенного ПО;

4.17.10. Техническое обслуживание должно осуществляться только на основании зарегистрированного обращения системного администратора;

4.17.11. Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя;

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

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

4.18.14. 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;

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

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

4.17.17. АРМ, на которых предполагается обрабатывать информацию ограниченного доступа, должны быть закреплены за соответствующим муниципальным служащим Администрации Зубцовского района. Запрещается использование указанных АРМ другими пользователями без согласования с системным администратором. При передаче указанного АРМ другому

пользователю должна производиться гарантированная очистка диска (форматирование)

4.17.18. Главный специалист, системный администратор Администрации Зубцовского района отказывается в устранении проблемы, вызванной наличием на рабочем месте ПО или оборудования, установленного или настроенного пользователем с нарушением действующей процедуры.

4.18. Порядок сопровождения ИС Администрации Зубцовского района.

Обеспечение ИБ на стадиях жизненного цикла (далее - ЖЦ) ИС должно осуществляться на всех его стадиях, автоматизирующих технологические процессы с учетом всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и контрольных органов Администрации Зубцовского района). Разработка технических заданий, проектирование, создание, тестирование, приемка средств и систем защиты ИС проводится при участии системного администратора. При разработке ИС необходимо придерживаться требований и методических указаний, определенных стандартами, входящими в группу ГОСТ 34 «Стандарты информационной технологии».

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

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 J решений; внесения разработчиком дефектов на уровне архитектурных решений; Г d внесения разработчиком недокументированных возможностей в ИС; неадекватной (неполной, противоречивой, некорректной и пр.) реализации требований к ИС; разработки некачественной документации; сборки ИС разработчиком/производителем с нарушением требований, что приводит к появлению недокументированных возможностей в ИС либо к неадекватной реализации требований; неверного конфигурирования ИС; приемки ИС, не отвечающей требованиям заказчика; внесения недокументированных возможностей в ИС в процессе проведения приемочных испытаний посредством недокументированных возможностей функциональных тестов и тестов ИБ.

Привлекаемые для разработки и (или) производства средств и систем защиты ИС на договорной основе специализированные организации должны иметь лицензии на данный вид деятельности в соответствии с законодательством Российской Федерации.

При приобретении готовых ИС и их компонентов разработчиком должна быть - Доставлена документация, содержащая;, в том числе, описание защитных мер, предпринятых разработчиком в отношении угроз ИБ.

Также разработчиком должна быть представлена документация, содержащая описание защитных мер, предпринятых разработчиком ИС, и их компонентов, Дающихся безопасности разработки, безопасности поставки, эксплуатации, поддержки ЖЦ, включая описание модели ЖЦ, 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 включаются положения по сопровождению поставляемых модулей на весь срок их службы. В случае невозможности включения в договор (контракт) указанных требований к разработчику, должна быть рассмотрена возможность приобретения полного комплекта рабочей документации на модуль для обеспечения последующего сопровождения ИС и их компонентов без участия разработчика. Если оба указанных, варианта неприемлемы, например, вследствие высокой цены, Администрация Зубцовского района должна провести анализ влияния угрозы невозможности сопровождения ИС и их компонентов на обеспечение непрерывности технологического процесса.

На стадии эксплуатации должна быть обеспечена защита от следующих угроз: умышленное несанкционированное раскрытие, модификация или уничтожение информации; неумышленная модификация или уничтожение информации; недоставка или ошибочная доставка информации; отказ в обслуживании или ухудшение обслуживания.

Кроме этого, актуальной является угроза отказа от авторства сообщения. На стадии сопровождения должна быть обеспечена защита от угроз: внесение изменений в ИС, приводящих к нарушению ее функциональности либо к появлению недокументированных возможностей; невнесение 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 Зубцовского района, и информации, используемой средствами обеспечения ИБ, из постоянной памяти или с внешних носителей.

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

4.19. Профилактика нарушений системы мероприятий ИБ

Под профилактикой нарушений системы мероприятий понимается проведение регламентных работ по защите информации, предупреждение

возможных нарушений ИБ в Администрации Зубцовского района и проведение разъяснительной работы по ИБ среди пользователей Администрации Зубцовского района.

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

Задача предупреждения в ИС Администрации Зубцовского района возможных крушений ИБ решается по мере наступления следующих событий: включение в состав ИС Администрации Зубцовского района новых программных и технических средств (новых рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС Администрации Зубцовского района; изменение конфигурации программных и технических средств ИС Администрации Зубцовского района (изменение конфигурации ПО рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС Администрации Зубцовского района; появление сведений о выявленных уязвимых местах в составе ОС и/или ПО технических средств, используемых в ИС Администрации Зубцовского района.

Системный администратор, в том числе используя рекомендации организации, специализирующейся в области ИБ и имеющей соответствующие сертификаты Федеральной службы по техническому и экспортному контролю (далее - ФСТЭК), собирает и анализирует информацию о выявленных уязвимых местах в составе ОС и/или ПО относительно ИС Администрации Зубцовского района. Источниками подобного рода сведений могут служить официальные издания и публикации в средствах массовой информации, общественных объединений и других организаций, специализирующихся в области защиты информации.

Системный администратор, в том числе используя рекомендации организации, специализирующейся в области ИБ и имеющей соответствующие сертификаты ФСТЭК, организует периодическую проверку СЗИ ИС Администрации Зубцовского района 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 Зубцовского района средств и функций защиты. По результатам профилактических работ, проводимых в ИС Администрации Зубцовского района, необходимо сделать соответствующие записи в Журнале проверки исправности и технического обслуживания.

Плановая разъяснительная работа, по правилам системы мероприятий ИБ, а также инструктаж служащих Администрации Зубцовского района по соблюдению требований нормативных и регламентных документов но ИБ, принятых в администрации Зубцовского района, проводятся системным администратором.

Неплановая разъяснительная работа, по правилам системы мероприятий ИБ, а также инструктаж сдужащих Администрации; Зубцовского района по соблюдению требований нормативных и регламентных документов по ИБ, принятых в Администрации Зубцовского района, проводятся при пересмотре системы мероприятий ИБ, при возникновении инцидента нарушения правил системы мероприятий.

Прием на работу служащих должен сопровождаться ознакомлением их с правилами и требованиями системы мероприятий.

4.20. Ликвидация последствий нарушения системы мероприятий ИБ

Системный, администратор, используя данные, полученные в результате применения инструментальных средств: контроля (мониторинга) безопасности информации ИС Администрации Зубцовского района, должен своевременно обнаруживать нарушения ИБ, факты осуществления НСД к защищаемым информационным ресурсам, и предпринимать меры по их. локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения ИБ или осуществления НСД к защищаемым информационным ресурсам ИС - Администрации Зубцовского района. рекомендуется уведомить системного администратора и далее следовать его указаниям.

Действия системного администратора.при признаках нарушения системы мероприятий ИБ регламентируются следующими документами: Политикой ИБ; инструкцией пользователя АС; должностной инструкцией системного администратора.

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

4.21. Ответственность нарушителей систем мероприятий ИБ

Ответственность за выполнение правил систем мероприятий безопасности несет, каждый служащий Администрации Зубцовского района в рамках своих служебных обязанностей и полномочий.

ЖУРНАЛ
проведения инструктажей по информационной
безопасности

Начат

Окончен

№ п/п	Дата проведения инструктажа	ФИО инструктируемого сотрудника	Вид инструктажа (первичный, на рабочем месте, повторный, индивидуальный)	Должность, ФИО, проводившего инструктаж	Подниеь \ инструктирующего \	инструктируемого \