ПРОЕКТ

Администрация Белозерского района

Курганской области

ПОСТАНОВЛЕНИЕ

от «\_\_\_» 2018 года № \_\_\_\_\_

 с. Белозерское

**Об утверждении Политики обеспечения информационной безопасности в Администрации Белозерского района**

В соответствии с Федеральным законом Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в целях обеспечения информационной безопасности автоматизированных информационных систем, используемых в Администрации Белозерского района, Администрация Белозерского района

ПОСТАНОВЛЯЕТ:

1. Утвердить Политику обеспечения информационной безопасности в Администрации Белозерского района согласно приложению к настоящему постановлению.

2. Руководителям структурных подразделений Администрации Белозерского района при создании и эксплуатации автоматизированных информационных систем обеспечить выполнение положений настоящего постановления.

3. Контроль за выполнением настоящего постановления оставляю за собой.

Первый заместитель

Главы Белозерского района А.В. Завьялов

|  |  |
| --- | --- |
|  | Приложениек постановлению Администрации Белозерского района от «\_\_\_» \_\_\_\_\_\_\_\_\_ 2018 года № \_\_\_«Об утверждении Политики обеспечения информационной безопасности в Администрации Белозерского района» |

**ПОЛИТИКА**

**обеспечения информационной безопасности**

**в Администрации Белозерского района**

**Раздел I. Общие положения**

**1. Назначение Политики обеспечения информационной безопасности в Администрации Белозерского района (далее – Политика).**

Настоящая Политика определяет систему взглядов на проблему обеспечения комплексной безопасности информации и устанавливает порядок организации и правила обеспечения информационной безопасности в Администрации Белозерского района и ее структурных подразделениях (далее - АМР), распределение функций и ответственности за обеспечение информационной безопасности между подразделениями и сотрудниками АМР, требования по информационной безопасности к информационным средствам, применяемым в АМР.

Документ представляет собой методологическую основу для разработки и реализации комплексных целевых программ обеспечения защиты информации на объектах информатизации АМР.

**2. Сфера применения Политики.**

Требования настоящей Политики обязательны для всех структурных подразделений АМР и распространяются на:

- автоматизированные системы АМР;

- средства телекоммуникаций;

- помещения;

- специалистов АМР.

Внутренние документы АМР, затрагивающие вопросы, рассматриваемые в данном документе, должны разрабатываться с учетом положений настоящего документа и не противоречить ему.

**3. Правовая основа Политики.**

Правовую основу Политики составляют:

- Конституция Российской Федерации;

- Федеральный закон от 28.12.2010 г. № 390-ФЗ «О безопасности»;

- Федеральный закон от 07.07.2003 г. № 126-ФЗ «О связи»;

- Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне»;

- Федеральный закон от 26.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Доктрина информационной безопасности Российской Федерации, утверждена Президентом Российской Федерации 09.09.2000 г. Пр-1895;

- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные приказом Гостехкомиссии России от 30.08.2002 г. № 282;

- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

- ГОСТ Р ИСО/МЭК 27002-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности (утв. и введен в действие приказом Росстандарта от 24.09.2012 г. № 423-ст);

- другие законодательные акты, руководящие и нормативно-методические документы Российской Федерации в области обеспечения информационной безопасности.

**Раздел II. Термины и определения**

**Аутентификация** - проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

**Администратор защиты** - субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

**Безопасность информации** - состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

**Доступ к информации** - ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

**Защита информации (ЗИ)** - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на информацию.

**Защита от несанкционированного доступа** - деятельность, направленная на предотвращение получения информации заинтересованным субъектом (или воздействия на информацию) с нарушением установленных прав или правил.

**Защищаемая информация** - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Защищаемые помещения** - помещения, специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, и т.п.).

**Информационные ресурсы** - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

**Идентификация** - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Идентификатор доступа** - уникальный признак субъекта или объекта доступа.

**Комплекс средств защиты** - совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации.

**Контролируемая зона** - пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание специалистов и посетителей администрации, а также транспортных средств.

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

**Несанкционированный доступ** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

**Нарушитель правил разграничения доступа** - субъект доступа, осуществляющий несанкционированный доступ к информации.

**Объект доступа** - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

**Организация защиты информации** - содержание и порядок действий по обеспечению защиты информации.

**Основные технические средства и системы** - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

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

**Система разграничения доступа** - совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах.

**Сертификат защиты** - документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и (или) распространение их как защищенных.

**Система защиты информации от несанкционированного доступа** - комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.

**Средство защиты от несанкционированного доступа** - программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

**Средство криптографической защиты информации** - реализующие алгоритмы криптографического преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для защиты информации, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи.

**Субъект доступа** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Целостность информации** - устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

**Раздел III. Цели и задачи обеспечения безопасности информации**

Основной целью, на достижение которой направлены положения Политики, является защита информации, содержащейся в информационных системах Администрации Белозерского района от наиболее распространенных угроз информационной безопасности, вызванных неэффективностью процедур контроля, технологических сбоев, несанкционированных действий специалистов или иных форм незаконного вмешательства в информационные ресурсы и информационные системы.

Указанная цель достигается посредством обеспечения и постоянного поддержания конфиденциальности, целостности и доступности информации.

Основными задачами обеспечения безопасности информации являются:

- оценка состояния информационной безопасности, прогнозирование и обнаружение угроз безопасности информации, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

- обеспечение соблюдения требований законодательства Российской Федерации в области информационной безопасности;

- организация и координация должностными лицами Администрации Белозерского района работ по обеспечению информационной безопасности;

- возложение ответственности за обеспечение безопасности информации в информационных системах на каждого сотрудника органа местного самоуправления в пределах его полномочий;

- обеспечение эффективной работы механизмов оперативного реагирования на компьютерные инциденты информационной безопасности;

 - ведение мониторинга состояния защищенности информации при ее обработке в информационных системах и защита от вмешательства в процесс функционирования информационной системы посторонних лиц;

- защиту конфиденциальной информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

- обеспечение работоспособности криптографических средств защиты информации;

- создание системы непрерывного обучения, тренировки и проверки осведомленности специалистов по вопросам обеспечения информационной безопасности;

- обеспечение защиты информации от несанкционированного доступа, предотвращение утраты, искажения или уничтожения информации на этапах сбора, обработки, хранения и предоставления конечному потребителю информации.

**Раздел VI. Объекты обеспечения информационной безопасности**

**4. Объекты защиты АМР.**

Объектами защиты АМР являются:

- информационные ресурсы;

- средства и системы обработки информации;

- средства и системы защиты информации, в т.ч. криптографической защиты информации;

- помещения или объекты, предназначенные для ведения закрытых переговоров.

**5. Информационные ресурсы АМР.**

Под информационными ресурсами в АМР понимаются совокупность сведений в электронном и бумажном виде (баз данных, электронных библиотек, реестров, кадастров, фондов, архивов и других видов информационных массивов), поддерживаемые программно-техническими средствами автоматизированной информационной системы. Информационные ресурсы представляют собой хранилища данных, из которого путем специализированной обработки пользователю предоставляется информация на электронных или бумажных носителях, в том числе в виде отдельных фрагментов баз данных, отчетов, выписок, справок.

Используемые в информационных системах АМР технологии взаимодействия при обработке информационных ресурсов включают:

- электронную почту;

- электронный обмен файлами;

- обмен файлами на магнитных носителях;

- web-доступ к ресурсам сети;

Основным источником информации для наполнения первичных баз данных ИТКС являются документы и сообщения, поступающие от структурных подразделений АМР и внешних организаций.

Вся информация, хранимая, обрабатываемая или передаваемая в рамках подразделений АМР с использованием информационной системы, классифицирована по степени важности и критичности на следующие категории:

1. Конфиденциальная информация.

К конфиденциальной относится информация, составляющая коммерческую тайну, информация о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющая идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях, а также любая другая закрытая информация, являющаяся собственностью АМР.

При обработке этой информации необходимо соблюдать специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные приказом Гостехкомиссии России от 30.08.2002 г. № 282, а также иные методические документы ФСТЭК России по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, от утечки по техническим каналам, положения Федерального закона № 152-ФЗ «О персональных данных», а также прочих нормативных правовых актов, регламентирующих работу с конфиденциальной информацией.

При хранении, передаче и обработке данной информации необходимо обеспечить максимальный уровень ее защиты.

1. Служебная информация.

К служебной информации могут быть отнесены любые сведения, относящиеся к деятельности подразделений АМР, несанкционированное распространение которых может привести к отрицательным экономическим, этическим или иным последствиям для АМР.

Хранение, обработка и передача такой информации должна осуществляться в соответствии с требованиями настоящего документа.

1. Рабочая информация.

Рабочая информация включает в себя сведения, имеющие отношение к внутренней деятельности подразделений АМР и не относящиеся к конфиденциальной или служебной информации.

При хранении, передаче и обработке такой информации необходимо обеспечить максимальный уровень ее целостности и аутентичности в соответствии с положениями настоящего документа.

1. Прочие виды информации.

Для прочих видов информации порядок хранения, передачи и обработки с использованием автоматизированных систем не регламентируется.

**6. Средства и системы обработки информации.**

Средства и системы обработки информации АМР представляют собой совокупность программного обеспечения и технических средств обработки и передачи информации, а также систему телекоммуникаций (далее - СТК).

Техническое обеспечение (далее - ТО) включает следующие компоненты:

- серверные комплексы (платформы);

- рабочие станции пользователей;

- технические средства ввода/вывода информации (сканеры, принтеры и т.п.);

- средства хранения и архивирования данных;

- активное и пассивное оборудование локальной вычислительной сети (ЛВС);

- средства бесперебойного питания.

Система телекоммуникаций (СТК) поддерживает информационный обмен между внутренними абонентами и информационными системами АМР, а также информационную связь с внешними абонентами.

В состав программного обеспечения информационных систем входят:

- общесистемное программное обеспечение;

- специальное (прикладное) программное обеспечение.

**7. Средства обеспечения.**

Под средствами обеспечения АМР понимаются вспомогательные инженерно-технические системы, не участвующие в обработке информации, содержащей конфиденциальные сведения. В общем виде к этим системам относятся:

- системы электропитания и заземления объектов;

- системы связи (ведомственной, междугородней, городской, внутренней), не предназначенной для закрытых переговоров;

- системы пожарной и охранной сигнализации;

- электронные системы контроля и управления доступом на территорию и в помещения;

- системы громкоговорящей связи и оповещения;

- системы кондиционирования, отопления и воздухоснабжения.

**8. Объекты, предназначенные для ведения закрытых переговоров.**

В качестве объектов, предназначенных для ведения закрытых переговоров или совещаний, необходимо рассматривать следующие помещения здания Администрации Белозерского района:

- кабинеты заместителей Главы Белозерского района, используемые для обсуждения конфиденциальной информации;

- зал заседаний Администрации Белозерского района для проведения совещаний и переговоров по конфиденциальным вопросам;

- другие помещения, в том числе и технические, в которых может обсуждаться конфиденциальная информация.

**Раздел V. Основные направления деятельности**

**Администрации Белозерского района по обеспечению**

**информационной безопасности**

Деятельность по обеспечению информационной безопасности призвана способствовать снижению рисков от угроз в информационной сфере, повышению эффективности и устойчивости в управлении информационными ресурсами и системами.

Каждое структурное подразделение Администрации Белозерского района самостоятельно определяет для себя основные направления деятельности по обеспечению информационной безопасности в зависимости от выполняемых функций и полномочий.

К основным направлениям деятельности Администрации Белозерского района по обеспечению информационной безопасности относятся:

- регламентация доступа в служебные помещения Администрации Белозерского района;
 - разграничение доступа к техническим средствам и информационным ресурсам Администрации Белозерского района;

- применение антивирусной защиты;

- применение криптографической защиты информации;

- применение обезличивания персональных данных;

- регламентация использования электронной почты;

- регламентация работы в сети Интернет;

- проведение внутреннего контроля и обучение служащих.

**9. Регламентация доступа в служебные помещения Администрации** **Белозерского района.**

Регламентация доступа в служебные помещения Администрации Белозерского района осуществляется в целях:

- обеспечения физической сохранности носителей информации, оборудования;
 - исключения возможности несанкционированного доступа в служебные помещения, в том числе, в которых ведется обработка конфиденциальной информации.
 Доступ служащих и посетителей в здание Администрации Белозерского района должен осуществляется в соответствии с Инструкцией об организации пропускного и внутриобъектового режима в Администрации Белозерского района, утверждаемого распоряжением Администрации Белозерского района.
 Доступ в помещения, в которых ведется обработка персональных данных, осуществляется в соответствии с Порядком доступа в помещения Администрации Белозерского района, в которых ведется обработка персональных данных, утверждаемого постановлением Администрации Белозерского района.

**10. Разграничение доступа к техническим средствам и информационным ресурсам Администрации Белозерского района.**

Разграничение доступа к техническим средствам и информационным ресурсам Администрации Белозерского района направлено на предотвращение получения информации, обрабатываемой в электронном виде, в том числе в информационных системах, с нарушением регламентируемых нормативными правовыми актами или владельцами информации правил, следствием которых может быть нарушение конфиденциальности, целостности и (или) доступности информации.
 Для работы с информационными ресурсами Администрации Белозерского района служащему предоставляется автоматизированное рабочее место (далее - АРМ).
ПО АРМ устанавливается и обновляется системным администратором со специальных ресурсов или съемных носителей в соответствии с лицензионным соглашением. При передаче АРМ другому служащему производится удаление профиля пользователя АРМ.
 Доступ к конфиденциальной информации, в том числе персональным данным, осуществляется в соответствии с Положением по организации работ по обеспечению безопасности конфиденциальной информации при её обработке в информационных системах Администрации Белозерского района, утвержденным постановлением Администрации Белозерского района от 14.12.2016 г. № 634. Обработка персональных данных осуществляется с особенностями, установленными Правилами обработки персональных данных в Администрации Белозерского района, утвержденными постановлением Администрации Белозерского района от 01.12.2015 г. № 590. К работе с информационными ресурсами Администрации Белозерского района допускаются служащие, ознакомленные с настоящей Политикой.

Для защиты своих паролей служащие обязаны:

- соблюдать конфиденциальность пароля - не сообщать пароль другим лицам, в том числе другим служащим, не хранить пароли в легкодоступных местах;

- выбирать трудно угадываемый;
 - использовать в пароле не менее 8 символов;
 - в случае компрометации пароля немедленно изменить пароль.
 Служащим запрещается самостоятельно устанавливать на АРМ дополнительные технические средства и (или) ПО.

**11. Антивирусная защита**

Антивирусная защита в Администрации Белозерского района применяется с целью защиты информационных ресурсов и ПО от несанкционированных действий (утраты, модификации, изменения) путем внедрения в информационную среду вирусов, вредоносных программ (далее - вирус) посредством использования специализированного ПО (далее - антивирусное ПО).

Антивирусное ПО должно быть развернуто на всех технических средствах, подверженных воздействию вирусов (АРМ, серверах). Антивирусные механизмы должны быть актуальными, постоянно включенными. Отключение антивирусного ПО или отказ от автоматического обновления антивирусных баз не допускается.
 Обязанность по установке и регулярному обновлению антивирусного ПО, в том числе антивирусных баз, на АРМ и серверах отраслевых органов Администрации Белозерского района возлагается на соответствующих системных администраторов. Для исключения заражения вирусами и обеспечения надежного хранения информации в электронном виде служащие обязаны:

- убедиться, что на АРМ установлено и включено антивирусное ПО;
 - незамедлительно сообщить системному администратору о нарушениях работы антивирусного ПО;

 - перед использованием проверять съемные носители информации на наличие вирусов средствами установленного на АРМ антивирусного ПО;

 - при переносе на свой АРМ файлов в архивированном виде проверять их до и после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами;

- использовать антивирусное ПО для входного контроля всех файлов (исполняемых файлов, файлов данных, сообщений электронной почты и так далее), получаемых из компьютерных сетей, а также на съемных носителях информации;
 - в случае установки или изменения ПО при возникновении подозрения на наличие вирусов проверять на наличие вирусов жесткие диски АРМ, запуская антивирусное ПО для тестирования файлов, памяти и системных областей дисков.
 При возникновении подозрения на наличие вирусов служащие обязаны:
 - приостановить все операции, связанные с обработкой файлов на АРМ;
 - запустить антивирусное ПО для тестирования файлов, памяти и системных областей дисков;

 - о факте обнаружения вирусов немедленно сообщить системному администратору, владельцам зараженных или поврежденных вирусами файлов, другим пользователям, использующим зараженные файлы в работе;

 - провести анализ необходимости дальнейшего использования зараженных вирусом файлов;

- провести самостоятельно или совместно с системным администратором лечение зараженных файлов, в случае обнаружения не поддающегося лечению вируса удалить инфицированный файл и проверить работоспособность компьютера.

 **12. Криптографическая защита информации**

Криптографическая защита информации (шифрование) применяется для обеспечения конфиденциальности информации при хранении в ненадежных хранилищах и (или) передаче ее по незащищенным каналам связи (телефон, факс, электронная почта и так далее). Шифрование осуществляется перед отправкой данных по незащищенным каналам связи или перед помещением на хранение в ненадежных хранилищах.

**13. Обезличивание персональных данных**

Обезличивание персональных данных в Администрации Белозерского района проводится в целях обеспечения защиты от несанкционированного распространения персональных данных при размещении в информационных системах, не предназначенных для обработки персональных данных (далее - открытые информационные системы), и (или) передаче по незащищенным каналам связи. Работа с обезличенными данными должна осуществляться в соответствии с Правилами работы с обезличенными персональными данными, обрабатываемыми в администрации Белозерского района, утвержденными постановлением Администрации Белозерского района от 15.12.2015 г. № 629. Обезличивание персональных данных должно производиться перед внесением их в открытую информационную систему и (или) передачей по незащищенным каналам связи.

**14. Регламентация использования электронной почты**

Система электронной почты Администрации Белозерского района (далее - электронная почта) используется в информационных целях, в том числе оповещения, организации работы, обеспечения внутренних и внешних коммуникаций. Регламентация использования электронной почты осуществляется с целью снижения риска умышленной или неумышленной несанкционированной рассылки информации, заражения информационных ресурсов Администрации Белозерского района вирусами.
 При работе с электронной почтой служащие обязаны:
 - перед отправкой письма тщательно проверять на отсутствие в нём персональных данных;

- периодически удалять из электронного почтового ящика ненужные сообщения и перемещать необходимые сообщения в архивные почтовые папки;
 - проверять сообщения электронной почты на наличие вирусов;

- использовать шифрование, обезличивание конфиденциальной информации при ее отправке.

**15. Регламентация работы в сети Интернет**

Сеть Интернет в Администрации Белозерского района используется служащими для получения информации в рамках исполнения должностных обязанностей.
 Регламентация работы в сети Интернет осуществляется с целью снижения риска заражения информационных ресурсов Администрации Белозерского района вирусами. Организацию доступа к сети Интернет для нужд Администрации Белозерского района осуществляет системный администратор. Доступ к сети Интернет предоставляется служащим с АРМ, закрепленным за служащим для исполнения должностных обязанностей.
 Угрозы, связанные с работой в сети Интернет:

- легкость перехвата данных и фальсификации IP-адресов в сети Интернет;
 - заражение вирусами.

Муниципальным служащим Администрации Белозерского района запрещается:

- осуществлять действия, запрещенные законодательством Российской Федерацией;
 - отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО;

- распространять информацию, содержащую подрывные, оскорбительные, неэтичные, незаконные материалы, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возраста, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений, национального происхождения, гиперссылки или другие ссылки на веб-сайты, содержащие указанные материалы, массовые рассылки спама;

- самостоятельно устанавливать на АРМ дополнительное ПО, полученное в сети Интернет;

- загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным ПО;

- открывать страницы сайтов, если имеются сомнения в надежности сайта и (или) имеются уведомления о возможном заражении вирусами;

Служащие обязаны при обнаружении попыток несанкционированного доступа и (или) при подозрении на наличие вируса немедленно прекратить работу в сети Интернет и сообщить системному администратору.

Доступ к сети Интернет может быть блокирован системным администратором без предварительного уведомления служащего при возникновении угрозы безопасности информации.

**Раздел VI. Принципы формирования системы обеспечения информационной безопасности в Администрации Белозерского района**

Построение системы обеспечения информационной безопасности в Администрации Белозерского района и ее функционирование осуществляется в соответствии с основными принципами формирования системы обеспечения информационной безопасности.

К основным принципам формирования системы обеспечения информационной безопасности в Администрации Белозерского района относятся:

**законность** – предполагает разработку системы обеспечения информационной безопасности в соответствии с действующим законодательством Российской Федерации в данной области с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией. Все пользователи информационных систем должны иметь представление об ответственности за правонарушения в области обеспечения информационной безопасности;

**системность** – предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, имеющих существенное значение для понимания и решения проблемы обеспечения информационной безопасности. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем, а также характер, возможные объекты и направления атак на них со стороны нарушителей, пути проникновения в информационные системы и несанкционированного доступа к информации;

**централизация управления** – предполагает, что деятельность по обеспечению информационной безопасности должна быть встроена в управленческие процессы Администрации Белозерского района, подчиняться понятным руководителям закономерностям и оцениваться с позиций эффективности, для этого процессы обеспечения информационной безопасности должны быть организованы и управляемы;

**персональная ответственность** – предполагает возложение персональной ответственности на каждого сотрудника, муниципального служащего в пределах его должностных полномочий за несоблюдение регламентирующих документов в области обеспечения информационной безопасности;

**минимизация полномочий** – предполагает предоставление прав доступа сотрудникам к информационным ресурсам в том случае и объеме, необходимом для качественного выполнения своих служебных (трудовых) обязанностей;

**своевременность** – предполагает своевременность выявления проблем, связанных с обеспечением информационной безопасности, и обнаружение угроз безопасности информации, потенциально способных нанести ущерб;

**комплексный подход** – предполагает всестороннее обеспечение информационной безопасности и предусматривает использование взаимоувязанных программно-технических, организационных, правовых мер обеспечения информационной безопасности на единой концептуальной основе;

**непрерывность** – предполагает непрерывный, целенаправленный процесс по выявлению угроз информационной безопасности и принятию адекватных мер защиты руководством и сотрудниками Администрации Белозерского района;

**совершенствование** – предполагает постоянное совершенствование мер и средств защиты информации на основе модернизации организационных и технических решений, кадрового состава, анализа функционирования информационной системы и системы ее защиты с учетом изменений в методах и средствах перехвата информации, обязательных требований по защите информации;

**взаимодействие и сотрудничество** – предполагает создание благоприятной атмосферы в коллективах структурных подразделений. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности ответственных за обеспечение информационной безопасности. Все сотрудники должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе;

**гибкость системы защиты** – система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления Администрацией Белозерского района своих полномочий. В число таких изменений входят изменения организационной и штатной структуры, изменение существующих или внедрение принципиально новых информационных систем, технических средств;

**обоснованность и техническая реализуемость** – информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по информационной безопасности;

**обязательность контроля** – предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения информационной безопасности. Выявленные недостатки системы обеспечения информационной безопасности должны немедленно доводиться до сведения Главы Белозерского района, а также оперативно устраняться.

**Раздел VII. Требования к организации обеспечения безопасности**

**информационных систем**

Обеспечение безопасности информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы (подсистемы) защиты информации информационной системы.

Для обеспечения безопасности информации, содержащейся в информационной системе, проводятся следующие мероприятия:

- формирование требований к защите информации, содержащейся в информационной системе;

- разработка и внедрение системы защиты информации информационной системы;

- аттестация информационной системы по требованиям защиты информации и ввод ее в действие;

- обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

- обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

Для проведения работ по обеспечению безопасности информации в ходе создания и эксплуатации информационной системы обладателем информации (заказчиком) в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

**Раздел VIII. Ответственные за обеспечение информационной безопасности в Администрации Белозерского района.**

Структурные подразделения Администрации Белозерского района, муниципальные учреждения принимают меры защиты информации и несут ответственность за выполнение требований настоящей Политики и документов, регламентирующих информационную безопасность, действующих на ее основе.

В Администрации Белозерского района должностным лицом, ответственным за непосредственную организацию и эффективное функционирование системы обеспечения информационной безопасности является заместитель Главы Белозерского района, управляющий делами на которого возлагается решение следующих основных задач:

- анализ текущего состояния обеспечения информационной безопасности в Администрации Белозерского района;

- организация мероприятий и координация работ всех подразделений по обеспечению информационной безопасности;

- контроль и оценка эффективности принятых мер и применяемых средств защиты информации.

Основные функции ответственного лица по обеспечению информационной безопасности заключаются в следующем:

- формирование требований к системе обеспечения информационной безопасности в процессе создания и дальнейшего развития существующих компонентов информационной системы;

- участие в проектировании системы обеспечения информационной безопасности, ее испытаниях и вводе в эксплуатацию;

- обеспечение функционирования системы защиты информации и ее элементов, включая управление криптографическими системами;

- обучение пользователей и обслуживающего персонала правилам обработки информации;

- оказание методической помощи сотрудникам в вопросах обеспечения информационной безопасности;

- контроль за соблюдением пользователями и обслуживающим персоналом установленных правил обращения с конфиденциальной информацией;

- организация по указанию Главы Белозерского района служебного расследования по фактам нарушения правил обращения с конфиденциальной информацией и оборудованием;

- принятие мер при попытках несанкционированного доступа к информационным ресурсам и компонентам системы или при нарушениях правил функционирования системы защиты;

- участие в работе по выявлению и устранению компьютерных инцидентов информационной безопасности.

**Раздел VIII. Основные организационные, технические и правовые меры**

**обеспечения безопасности информации**

Для организации и внедрения системы защиты информации в информационной инфраструктуре Администрации Белозерского района важное значение имеет анализ технических, структурных, эксплуатационных и иных особенностей информационных систем, используемых технологий и архитектурных решений.

Все меры обеспечения безопасности информационных систем Администрации Белозерского района подразделяются на правовые (законодательные), организационные, технические и физические, а также применение криптографических методов и средств защиты информации, необходимых для обеспечения информационной безопасности.

**16. Правовые (законодательные) меры обеспечения безопасности информационных систем.**

К правовым (законодательным) мерам обеспечения безопасности информационных систем относятся действующие в Российской Федерации правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения принятых в них правил.

Следует учитывать, что лица, виновные в нарушении обязательных требований по обеспечению информационной безопасности несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационной системы.

**17. Организационные меры обеспечения безопасности информационных систем.**

Организационные меры обеспечения безопасности информационных систем - меры организационного характера, регламентирующие процессы функционирования информационных систем, использование их ресурсов, деятельность обслуживающего персонала, а также порядок обращения пользователей информации с информационными системами таким образом, чтобы в наибольшей степени затруднить либо исключить возможность реализации угроз информационной безопасности, снизить размер потерь в случае реализации угроз.

**18. Технические меры обеспечения безопасности информационных систем.**

Технические меры обеспечения безопасности информационных систем должны быть основаны на использовании единых программных и технических средств, входящих в состав информационных систем и выполняющих самостоятельно или в комплексе с другими средствами функции защиты.

Технические меры обеспечения безопасности информационных систем реализуются, в том числе посредством применения средств защиты информации, прошедших оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации. Данный перечень размещен на официальном сайте ФСТЭК России (www.fstec.ru).

Применение организационных и технических мер защиты информации, реализуемых в информационных системах в рамках их систем защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационных систем должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;

- управление доступом субъектов доступа к объектам доступа;

- ограничение программной среды;

- защиту машинных носителей информации;

- регистрацию событий безопасности;

- антивирусную защиту;

- обнаружение вторжений;

- контроль (анализ) защищенности информации;

- обеспечение целостности информационной системы и информации;

- обеспечение доступности информации;

- защиту технических средств;

- защиту информационной системы, ее средств, систем связи и передачи данных, в том числе, посредством применения активных и пассивных средств защиты информации, обрабатываемой техническими средствами информационных систем и циркулирующей в помещениях объекта от утечки по техническим каналам.

Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой информационной системой, должны быть направлены на обеспечение конфиденциальности, целостности и доступности информации.

**19. Криптографические методы и средства защиты.**

Криптографические методы и средства защиты (далее – СКЗИ) используются для обеспечения информационной безопасности. Организация в Администрации Белозерского района системы информационной безопасности на основе инфраструктуры с использованием СКЗИ позволит решить задачи:

- организации обеспечения защищенного документооборота с использованием имеющихся систем, как внутри, так и при взаимоотношениях с другими организациями. Это позволит повысить эффективность и снизить накладные расходы на администрирование системы и использовать единые стандарты защиты данных;

- реализации централизованно-контролируемой системы информационной безопасности, при этом гибкой и динамически управляемой;

- универсализации методов обеспечения доступа пользователей и защиты для системы электронной почты, системы доступа в МКС «Интернет» и других систем с использованием уже имеющихся в этих приложениях механизмов обеспечения информационной безопасности;

- использования имеющихся реализаций российских криптографических алгоритмов в операциях с сертификатами и при защите электронного документооборота.

Использование СКЗИ для обеспечения безопасности информации необходимо в случаях, если:

- информация подлежит криптографической защите в соответствии с законодательством Российской Федерации;

- в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью данных средств (передача информации по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче информации, содержащей сведения конфиденциального характера, по информационно-телекоммуникационным сетям общего пользования; хранение информации на носителях, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов).

**20. Физические меры защиты.**

Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации. Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в них посторонних лиц, хищение документов и носителей информации, самих средств информатизации, а также исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств съема информации.

**Раздел X. Обучение специалистов и повышение осведомленности в вопросах**

**обеспечения информационной безопасности**

Подготовка и переподготовка пользователей и специалистов АМР по защите информации требует создания системы повышения уровня технической грамотности и информированности пользователей в области информационной безопасности, а также переподготовки специалистов по защите информации.

Для этого необходимо регулярно проводить тренинги для персонала и контроль готовности новых специалистов по применению правил информационной защиты, а также периодически осуществлять переподготовку специалистов Администрации Белозерского района, ответственных за защиту информации.

Особенно важно проводить тренинги при изменении конфигурации информационной системы (внедрении новых технологий и прикладных автоматизированных систем, смены оборудования, операционной системы, ключевых приложений, принятии новых правил или инструкций и т.д.).

Все пользователи информационной системы должны быть ознакомлены с организационно - распорядительными документами Администрации Белозерского района по обеспечению информационной безопасности, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности информации. Доведение требований указанных документов до лиц, допущенных к обработке защищаемой информации, осуществляется под подпись системными администраторами. Пользователи информационной системы, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки конфиденциальной информации.

Целью обучения специалистов является, снижение потерь (материальных, финансовых, ущерб репутации и т.д.) от угроз, связанных с незнанием или непониманием основных положений законодательства Российской Федерации в области обеспечения информационной безопасности и правил по защите информации.

Задачи повышения осведомленности специалистов в вопросах информационной безопасности:

- информирование специалистов о существующих угрозах и проблемах информационной безопасности, которые могут возникнуть при автоматизированной обработке информации, обновление их теоретических и практических знаний в области обеспечения информационной безопасности;

- доведение до специалистов основных положений, ограничений и требований существующих нормативно-распорядительных документов принятых в Администрации Белозерского района;

- выработка у специалистов умения оценивать возможные последствия своих действий (адекватно оценивать связанные с ними риски информационной безопасности);

- выработка у специалистов привычек, способствующих поддержанию высокого уровня информационной безопасности;

- выработка у специалистов ОМСУ умений (навыков) правильно и оперативно действовать при возникновении инцидентов информационной безопасности;

- доведение до специалистов их обязанностей в области обеспечения информационной безопасности и степени их ответственности в случае утечки конфиденциальной информации;

Формы и методы повышения осведомленности муниципальных служащих в области информационной безопасности:

- инструктаж при приеме на работу;

- повышение квалификации (курсы, семинары, тренинги);

- инструктажи и зачеты по положениям законодательства Российской Федерации в области обеспечения информационной безопасности и Политики;

- распространение кратких памяток, рассылки на электронную почту, разделы на сайте Администрации Белозерского района.

**Раздел XI. Контроль состояния информационной безопасности**

Контроль состояния информационной безопасности осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, за счет несанкционированного доступа к ней, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации, разрушение средств информатизации.

Основная задача контроля заключается в получении объективных оценок текущего состояния обеспечения информационной безопасности, оценка эффективности применяемых мер и технических решений для обеспечения информационной безопасности, оказание методической помощи по обеспечению защиты информации, организация работы по обеспечению информационной безопасности.

Внутренний аудит информационных систем АМР производится специалистами, ответственными за информационную безопасность, по распоряжению Главы Белозерского района.

Результаты аудита должны содержать отчеты по обеспечению безопасности информационной системы подразделения в целом или ее логических компонентов. Описания, выявленные факты и рекомендации, полученные в ходе проведения аудита, должны быть использованы для дальнейшей оценки защищенности информационной системы.

Проверки организации и состояния информационной безопасности могут быть:

- плановыми;

- внезапными;

- по фактам нарушения информационной безопасности.

 Плановые проверки проводятся в соответствии с годовым планом проверок, который составляется системным администратором Администрации Белозерского района на очередной год, утверждается Главой Белозерского района и рассылается во все структурные подразделения. В ходе плановых проверок должна полностью проверяться вся организация системы информационной безопасности подразделения.

Внезапные проверки проводятся в соответствии с внутренними планами работы. Внезапные проверки проводятся по отдельным вопросам организации информационной безопасности.

Проверки по фактам нарушения информационной безопасности проводятся после того, как нарушение устранено. Проверка проводится с целью выявления причин и предпосылок нарушения и выработки мер по предупреждению подобных нарушений в дальнейшем. Результаты всех проверок оформляются в виде актов с необходимыми в каждом конкретном случае приложениями.

Системные администраторы на подведомственных участках:

- контролируют правильность выполнения сотрудниками действий по доступу к объектам информационной системы;

- анализируют состояние информационной системы с целью выявления попыток несанкционированного доступа и использования информационных средств и информации;

- контролируют правильность использования имеющихся коллективных и индивидуальных средств информационной защиты.

В случае выявления каких-либо отклонений или нарушений в системе информационной безопасности администраторы безопасности принимают меры к их устранению самостоятельно или через руководителя соответствующего подразделения. Ответственность за принятие этих мер и сообщение о происшедшем ответственному лицу за информационную безопасность несет системный администратор.

Специалисты подразделения анализируют состояние своих рабочих мест с целью выявления попыток несанкционированного доступа и использования информационных средств и информации. В случае выявления таких попыток работник Администрации Белозерского района сообщают об этом системному администратору и руководителю структурного подразделения.

Список используемых сокращений:

|  |  |
| --- | --- |
| АИС | Автоматизированная информационная система |
| АРМ | Автоматизированное рабочее место |
| АС | Автоматизированная система |
| БД | База данных |
| ВТСС | Вспомогательные технические средства и системы |
| ЕСПД | Единая система программной документации |
| ЕСТД | Единая система технологической документации |
| ЗИ | Защита информации |
| ЗП | Защищаемое помещение |
| ИБ | Информационная безопасность |
| ИСПДн | Информационная система персональных данных |
| ИТКС | Информационно-телекоммуникационная система |
| КЗ | Контролируемая зона |
| КСЗИ | Комплексная система защиты информации |
| ЛВС | Локальная вычислительная сеть |
|  НСД | Несанкционированный доступ |
| ОБИ | Обеспечение безопасности информации |
| ОТСС | Основные технические средства и системы |
| ПОПолитика | Программное обеспечениеПолитики обеспечения информационной безопасности в Администрации Белозерского района |
| ПС | Программные средства |
| СКЗИ | Средство криптографической защиты информации |
| СПД | Система передачи данных |
| СПО | Специальное программное обеспечение |
| СТК | Система телекоммуникаций |
| СУБД | Система управления базами данных |
| ТП | Технический проект |
| ТТ | Технические требования |
| УЦ | Удостоверяющий центр |
| ФСБ России | Федеральная служба безопасности России |
| ФСТЭК России | Федеральная служба по техническому и экспертному контролю России |
| ЭЦП | Электронная цифровая подпись |

Заместитель Главы Белозерского района,

управляющий делами Н.П. Лифинцев