АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
« ВОХТОМСКОЕ»

ПОСТАНОВЛЕНИЕ

04.03.2024 № 14

п. Фоминский, Коношский район,
Архангельская область

Об утверждении Политики информационной безопасности в администрации муниципального образования «Вохтомское»

Руководствуясь требования Федерального закона от 27.07.25006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», администрация постановляет:

1. Утвердить Политику информационной безопасности в администрации муниципального образования «Вохтомское», приложение № 1.
2. Разместить Политику информационной безопасности на сайте администрации муниципального образования «Вохтомское» в информационно- телекоммуникационной сети «Интернет».
3. Настоящее постановление вступает в силу со дня его подписания.
4. Контроль за исполнением настоящего постановления оставляю за собой.

Глава муниципального
образования «Вохтомское» И.А.Нефедова

Приложение № 1
к Постановлению администрации
муниципального образования «Вохтомское»
от 04.03.2024 № 14

Политика информационной безопасности
в администрации муниципального образования «Вохтомское»

Определения

Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Информация - сведения (сообщения, данные) независимо от формы их представления.

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами.

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Конфиденциальная информация - обязательные для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким- либо признакам.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

1. Общие положения

1.1. Настоящая Политика информационной безопасности в администрации муниципального образования «Вохтомское» (далее – администрация) определяет основные принципы, направления и требования по защите информации, является основным внутренним документом для обеспечения режима информационной безопасности, служит руководством при разработке соответствующих Положений, Правил, Инструкций.

1.2. В рамках своей деятельности администрация обязуется предпринимать все возможные меры для защиты информации от риска причинения вреда, убытков и ущерба, возникающих в результате реализации угроз информационной безопасности или других противоправных действий, связанных с нарушением информационной безопасности администрации.

1.3. Настоящая Политика обязательна для применения всеми сотрудниками администрации.

2. Цели, задачи, принципы обеспечения информационной безопасности в администрации

2.1. Цели информационной безопасности:

- защита интересов администрации, работников и иных субъектов информационных отношений, взаимодействующих с администрацией, от возможного нанесения материального, физического, морального или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования

информационных систем администрации, нарушения работы технических и программных устройств, приводящего к недоступности информации, разглашению, искажению, уничтожению защищаемой информации и ее незаконному использованию;
- снижение угроз информационной безопасности до приемлемого уровня:
- защита персональных данных, обрабатываемых в информационных системах администрации;
- минимизация уровня рисков.
2.2. Основные задачи по обеспечению информационной безопасности:
- отнесение информации к категории несекретной, ограниченного распространения, коммерческого и другим видам тайн, иной конфиденциальной информации, информации персонального характера подлежит защите от неправомерного использования;
- прогнозирование и своевременное выявление угроз безопасности информационным ресурсам администрации, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;
- создание условий функционирования администрации с наименьшей вероятностью реализации угроз безопасности информационных ресурсов и нанесения ущерба;
- создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявление негативных тенденций в функционировании администрации, на основе нормативных, правовых, организационных и технических мер и средств обеспечении безопасности;
- создание условий для максимально возможного предотвращения и локализации ущерба, наносимого неправомерными действиями физических и (или) юридических лиц.
2.3. Принципы обеспечения информационной безопасности:
- **законности** – соблюдение действующего законодательства по защите информации, защите персональных данных, законных интересов всех участников информационного обмена, программно- технические средства, применяемые в администрации, должны иметь соответствующие лицензии, официально приобретаться у представителей разработчиков этих средств;
- **системности** - подход к вопросам организации информационной безопасности должен быть логическим и последовательным: в первую очередь категорирование обрабатываемой информации, информационной системы, оценка риска информационной безопасности исходя из реальных угроз и уязвимости информационных ресурсов, затем создание комплекса организационных и технических мер и средств защиты, учитывающих специфику администрации;
- **эффективности** - реализуемые в разумно достаточном объеме меры и мероприятия по обеспечению информационной безопасности должны сводить риски к приемлемому уровню, при этом адекватность и эффективность защитных мер должна быть оцениваема на регулярной основе;
- **целесообразности** - соблюдение соразмерности затрат на обеспечение защиты и информации и потенциальных потерь при реализации угрозы;
- **непрерывности** - принцип функционирования системы информационной безопасности, учитывающий, что злоумышленники в любой момент времени ищут возможность обхода защитных мер, прибегая для этого к легальным и нелегальным методам;
- **взаимодействии и координации** - при организации действий по обеспечению информационной безопасности администрация обеспечивает условия для эффективной координации и четкой взаимосвязи сотрудников между собой, с представителями сторонних организации, оказывающих услуги в рамках договорных обязательств;
- **совершенствовании** - совершенствование мер и средств защиты информации на основе собственного опыта, появления новых технических средств с учетом изменений в методах и средствах атак информационных ресурсов, нормативно - технических требований, достигнутого отечественного и зарубежного опыта;

- **приоритетности** - категорирование (ранжирование) информации и всех информационных ресурсов администрации по степени важности и оценка реальных, а также потенциальных угроз информационной безопасности;
- **персональной ответственности и разделения обязанностей** - определение прав и ответственности каждого конкретного работника (в пределах его должностных обязанностей) за обеспечение информационной безопасности.

3. Объекты информационной безопасности в администрации

3.1. Основные объекты защиты системы информационной безопасности:
- персональные данные, информационные ресурсы, обрабатывающие персональные данные, сведения ограниченного распространения, независимо от формы и вида их представления;
- информационные ресурсы, содержащие персональные данные;
- сотрудники администрации, являющиеся пользователями информационных ресурсов (систем) администрации;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы;
- программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) информационной системы администрации, с помощью которых производится обработка защищаемой информации;
- помещения, предназначенные для обработки персональных данных, сведений конфиденциального (персонального) характера);
- помещения, в которых расположены средства обработки защищаемой информации;
- технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация.

3.2. Подлежащая защите информация может находиться:
- на бумажных носителях;
- в электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники);
- передаваться по телефону, телефаксу и т.п.;
- записываться и воспроизводиться с помощью программных и технических средств (диктофоны, видеомагнитофоны и др.).

3.3. Среда информационного обмена обеспечивается, в том числе, общедоступными информационными ресурсами.

4. Угрозы информационной безопасности

4.1. Под угрозами информационной безопасности понимаются потенциально возможные негативные воздействия на защищаемую информацию, к числу которых относятся:
- несанкционированное распространением (передача) персональных данных;
- утрата сведений, составляющих конфиденциальную информацию, персональные данные администрации и иную защищаемую информацию, а также искажение такой информации;
- утечка - несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д.);
- недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, систем управления баз данных, воздействия вирусов, стихийных бедствий и иных форс- мажорных обстоятельств;

- отсутствие планирования и контроля;
- низкая степень надежности программного обеспечения;
- недостаточная осведомленность персонала, низкая квалификация персонала и пользователей в области информационных технологий.

4.2. В результате воздействия указанных угроз могут возникнуть следующие негативные последствия, влияющие на состояние информационной безопасности и нормального функционирования администрации:
- финансовые потери, связанные с утечкой или разглашением защищаемой информации;
- финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;
- ущерб от дезорганизации деятельности администрации и потери, связанные с невозможностью выполнения им своих обязательств;
- моральные потери (ущерб репутации администрации).

5. Меры обеспечения информационной безопасности

5.1. Требования об обеспечении информационной безопасности администрации и обработке персональных данных обязательны к соблюдению всеми сотрудниками администрации и пользователями информационных систем.

5.2. Система обеспечения безопасности информационных ресурсов должна соответствовать экономической целесообразности.

5.3. Система обеспечения безопасности информационных ресурсов должна предусматривать комплекс организационных, технических, криптографических, программных средств и мер по защите информации в процессе документооборота, при работе работников с персональными данными, конфиденциальными документами и сведениями, при обработке информации в информационных системах различного уровня и назначения, при передаче по каналам связи, при ведении деловых переговоров.

5.4. Управление рисками информационной безопасности в администрации включает в себя:
- анализ влияния на информационную безопасность администрации применяемых в деятельности администрации технологий, а также внешних по отношению к администрации событий;
- выявление проблем обеспечения информационной безопасности, анализ причин их возникновения и прогнозирования их развития;
- определение моделей угроз, выявление, анализ и оценка значимых для администрации угроз информационной безопасности;
- выявление возможных негативных рисков для администрации, наступающих в результате проявления рисков информационной безопасности, в том числе связанных с нарушением свойств безопасности информационных активов администрации;
- идентификацию и анализ рисковых событий информационной безопасности;
- оценку величины рисков информационной безопасности и выявление рисков, неприемлемых для учреждения;
- оценку влияния защитных мер на цели основной деятельности администрации;
- оценку затрат на реализацию защитных мер.

5.6. Организационные меры обеспечения информационной безопасности включают в себя:
- организацию контроля доступа в здание и помещения администрации, в т. ч., арендуемые помещения, предназначенные для обработки сведений конфиденциального и персонального характера;
- разработку и осуществление разрешительной системы допуска работников к работам с документами и персональными данными;
- заключение трудовых договоров и получение у работников добровольного согласия на соблюдение требований, регламентирующих режим информационной безопасности,

обработки персональных данных и сохранность конфиденциальной информации (персональных данных);
- установление единого порядка хранения и обращения персональных данных, конфиденциальной информации (носителей информации);
- координацию работ по защите информации, обрабатываемой и передаваемой средствами и системами вычислительной технике и связи;
- проведение периодического обучения и повышения квалификации работников администрации в области информационной безопасности;
- минимизацию данных конфиденциального (персонального) характера, доступных работникам;
- обеспечение физической сохранности автоматизированной системы и дополнительного оборудования;
- практическую проверку функционирования мер защиты обработки персональных данных и конфиденциальной информации.

5.7. Технические меры обеспечения информационной безопасности включают в себя:
- обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам информационных систем администрации и информации, обрабатываемой в них;
- применение программных, программно - аппаратных средств криптографической защиты информации;
- обеспечение бесперебойной работы информационной системы обработки персональных данных и сети связи;
- обеспечение возобновления работы информационных ресурсов и сети связи после прерываний и нештатных ситуаций;
- применение средств защиты от вредоносных программ;
- применение средств обнаружения вторжений;
- обеспечение информационной безопасности при использовании доступа в сеть «Интернет» и услуг электронной почты;
- предотвращения несанкционированного изменения программ и оборудования , контроль всех процедур, производимых с файлами на носителях и т.д.;
- проверку машинных и ручных протоколов выполнения работ со стороны пользователей;
- применение мер и технических средств, снижающих вероятность несанкционированного получения информации в устной форме (пассивная защита).

5.8. Управление инцидентами информационной безопасности в администрации включает в себя:
- сбор информации о событиях информационной безопасности;
- выявление и анализ инцидентов информационной безопасности;
- расследование инцидентов информационной безопасности;
- оперативное реагирование на инцидент информационной безопасности;
- минимизация негативных последствий инцидентов информационной безопасности;
- оперативное доведение до руководства администрации информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие ребшений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;
- выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки;
- пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности пол результатам рассмотрения инцидентов информационной безопасности.

6. Структура управления Политикой информационной безопасности

6.1. В целях выполнения задач по обеспечению информационной безопасности администрации, в администрации определены следующие субъекты информационных отношений:
- администрация, как собственник информационных ресурсов и оператор персональных данных;
- глава администрации, муниципальные служащие, как пользователи и поставщики информации в информационные системы;
- юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационных системах администрации.
6.2. Субъекты информационных отношений заинтересованы в обеспечении:
- конфиденциальности определенной части информации;
- целостности информации;
- своевременного доступа к необходимой им информации;
- защиты от навязывания им ложной (недостоверной, искаженной) информации;
- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;
- защиты соответствующей части информации от незаконного ее тиражирования и распространения.
6.3. Общее руководство по обеспечению информационной безопасности администрации осуществляет глава администрации.
6.4. Оперативная деятельность и планирование деятельности по обеспечению информационной безопасности администрации осуществляется и координируется ответственным за организацию информационной безопасности в администрации муниципального образования «Вохтомское».
6.5. Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы организации информационной безопасности администрации лежит на ответственном за организацию информационной безопасности в администрации муниципального образования «Вохтомское».
6.6. Сотрудники администрации:
- соблюдают и выполняют требования Политики информационной безопасности, соответствующих локальных актов, документов администрации по вопросам информационной безопасности;
- соблюдают конфиденциальность данных, доступ к которым был ими получен;
- обеспечивают физическую безопасность всего технического оборудования и носителей информации, используемых в работе;
- не допускают самовольного подключения и использования в автоматической информационной системе личного компьютерного и цифрового оборудования, а также носителей информации;
- не допускают самовольную установку программного обеспечения на компьютеры, входящие в состав информационной системы;
- своевременно информируют главу администрации о всех нарушениях информационной безопасности и о всех выявленных сбоях в работе программных и программно - аппаратных средств;
- проявляют осмотрительность в отношении любых действий, которые могут повлечь за собой снижение уровня информационной безопасности.
6.7. Сторонние физические и юридические лица:
- соблюдают и выполняют требования Политики информационной безопасности, соответствующих локальных актов и документов администрации по вопросам информационной безопасности при исполнении договорных обязательств.

6.8. Финансирование работ по реализации положений настоящей Политики осуществляется в рамках бюджета администрации муниципального образования «Вохтомское».

7. Заключение

7.1. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года. При внесении изменений в актуальной редакции указывается дата последнего обновления. Настоящая Политика подлежит размещению на официальном сайте администрации муниципального образования «Вохтомское» в информационно - телекоммуникационной сети «Интернет».

7.1. Общий контроль состояния информационной безопасности администрации осуществляет глава администрации.

7.2. Контроль исполнения требований настоящей Политики осуществляет ответственный за организацию информационной безопасности в администрации муниципального образования «Вохтомское».

7.3. Ответственность муниципальных служащих администрации муниципального образования «Вохтомское», имеющих доступ к конфиденциальной информации, за невыполнение требований норм, регулирующих обработку и защиту информации, определяется в соответствии с законодательством Российской Федерации и внутренними документами администрации муниципального образования «Вохтомское».

Лист ознакомления

с Политикой Политика информационной безопасности в администрации муниципального образования «Вохтомское»

№ п/п	ФИО	Должность	Дата	Подпись