АДМИНИСТРАЦИЯ
МОЛОТЫЧЕВСКОГО СЕЛЬСОВЕТА
ФАТЕЖСКОГО РАЙОНА

ПОСТАНОВЛЕНИЕ

от 14.02.2024г. **№ 11**

Об утверждении политики информационной безопасности Администрации Молотычевского сельсовета Фатежского района

В соответствии со статьями 6, 16 Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» Администрация Молотычевского сельсовета Фатежского района постановляет:

1. Утвердить прилагаемую Политику информационной безопасности Администрации Молотычевского сельсовета Фатежского района.

2. Контроль за выполнением настоящего постановления оставляю за собой.

3. Постановление вступает в силу со дня его подписания.

Г лава Молотычевского сельсовета Фатежского района О.М. Кретова

УТВЕРЖДЕНА
Постановлением Администрации Молотычевского
сельсовета Фатежского района
от 14.02.2024 г. № 11 «Об утверждении политики
информационной безопасности Администрации
Молотычевского сельсовета Фатежского района»

Политика
информационной безопасности Администрации Молотычевского сельсовета Фатежского района

I. Общие положения

1.1. Настоящая Политика инфсрмапионной безопасности Администрации Молотычевского сельсовета Фатежского района (далее - Политика ИБ) разработана в целях установления безопасных способов обработки информации в электронном виде, в том числе в информационных системах (сайтах) Администрации Молотычевского сельсовета Фатежского района (далее - информационная система).

1.2. Настоящая Политика ИБ определяет в Администрации Молотычевского сельсовета Фатежского района цели и задачи защиты информации, устанавливает методы защиты информации, которыми должны руководствоваться муниципальные служащие Администрации Молотычевского сельсовета Фатежского района, иные работники Администрации Молотычевского сельсовета Фатежского района, замещающие должности, не отнесенные к должностям муниципальной службы (далее - служащие), при обработке информации в электронном виде, в том числе в информационных системах, ответственность служащих за нарушение требований настоящей Политики ИБ.

Действие настоящей Политики ИБ не применяется к отношениям, связанным с обеспечением безопасности информации, составляющей государственную тайну.

1.3. Настоящая Политика ИБ применима ко всем техническим средствам (серверам, периферийному оборудованию, автоматизированным рабочим местам (далее - АРМ) и так далее), установленным в структурных подразделениях Администрации Молотычевского сельсовета Фатежского района, ко всем процессам обработки информации с использованием указанных технических средств, кроме технических средств, на которых обрабатывается информация, составляющая

государственную тайну (далее - объекты защиты).

1.4. Действие настоящей Политики ИБ распространяется на все структурные подразделения Администрации Молотычевского сельсовета Фатежского района. При осуществлении санкционированного доступа к информационным ресурсам Администрации Молотычевского сельсовета Фатежского района органами государственной власти, иными органами местного самоуправления, государственными, муниципальными учреждениями требования по безопасности информации устанавливаются в соглашении об информационном взаимодействии.

1.5. Правовыми основаниями настоящей Политики ИБ являются Конституция Российской Федерации, Гражданский кодекс Российской Федерации, Уголовный кодекс Российской Федерации, Кодекс Российской Федерации об административных правонарушениях, Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», иные нормативные правовые акты Российской Федерации, акты и документы Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности, Федеральной службы по надзору в сфере связи и массовых коммуникаций.

II. Термины и определения

В настоящей Политике ИБ используются следующие термины и определения:

вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения; вредоносная программа - компьютерная программа либо иная компьютерная информация, предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

доступность информации - состояние информации, при котором субъекты, имеющие санкционированные права доступа, могут реализовать их беспрепятственно; защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых актов или требованиями, устанавливаемыми собственником информации;

идентификатор (имя, логин) - набор символов, представляющий уникальное наименование объекта или субъекта в информационной системе, позволяющее однозначно идентифицировать пользователя при входе его в систему, определить его права в ней, фиксировать действия и тому подобное;

информационная безопасность - состояние защищенности информационной среды;

информационная среда - совокупность условий для технологической переработки и эффективного использования информационных ресурсов (в том числе технические средства, программное обеспечение, телекоммуникации, уровень подготовки пользователей, формы контроля, документопотоки, процедуры, регламенты, юридические нормы, иные факторы, воздействующие на информационные процессы и информационные системы);

информационные ресурсы - отдельные документы, массивы документов, в том числе содержащиеся в информационных системах (архивах, фондах, банках данных, других информационных системах); инцидент информационной безопасности - любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность;

несанкционированное действие - действие субъекта в нарушение установленных в информационной системе регламентируемых правил обработки информации;

оператор информационной системы Администрации Молотычевского сельсовета Фатежского района (далее - оператор информационной системы) - функциональный орган или структурное подразделение Администрации Молотычевского сельсовета Фатежского района, определяющий цели и порядок эксплуатации информационной системы;

пароль - конфиденциальная последовательность символов, связанная с субъектом и известная только ему, позволяющая его аутентифицировать, то есть подтвердить соответствие реальной сущности субъекта предъявляемому им при входе идентификатору;

профиль - набор установок и конфигураций, специфичный для данного субъекта или объекта и определяющий его работу в информационной системе;

системный администратор - лицо, обеспечивающее выполнение функций по обеспечению работы компьютерной техники, сети и программного обеспечения в структурном подразделении Администрации Молотычевского сельсовета Фатежского района;

угроза безопасности информации - потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному тиражированию, которое наносит ущерб собственнику, владельцу или пользователю информации;

уязвимость - свойство информационной системы, обусловливающее возможность реализации угроз безопасности, обрабатываемой в ней информации; целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими санкционированное право

на изменение информации.

Термины «информация, информационная система, информационная система персональных данных, конфиденциальность информации, обладатель информации, сайт в сети Интернет (далее - сайт), спам, обезличивание персональных данных, общедоступная информация» используются в значениях, установленных федеральными законами от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 10.09.2007 г. № 575 «Об утверждении Правил оказания телематических услуг связи».

Термины «электронная подпись, сертификат ключа проверки электронной подписи, владелец сертификата ключа проверки электронной подписи, ключ электронной подписи, ключ проверки электронной подписи, средства электронной подписи» используются в значениях, установленных Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».

III.Цели и задачи защиты информации в Администрации Молотычевского сельсовета Фатежского района, основные виды угроз безопасности информации

3.1. Обеспечение информационной безопасности в Администрации Молотычевского сельсовета Фатежского района (защита информации) - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и (или) непреднамеренных воздействий на защищаемую информацию, ее носители, процессы обработки. Защищаемой информацией в Администрации Молотычевского сельсовета Фатежского района является вся информация, обрабатываемая в Администрации Молотычевского сельсовета Фатежского района (структурных подразделениях) (далее - информация), независимо от ее местонахождения в информационной среде.

В Администрации Молотычевского сельсовета Фатежского района обрабатывается информация различных уровней конфиденциальности:

общедоступная (открытая) информация, для которой требуется обеспечение доступности и целостности;

информация ограниченного распространения, доступ к которой ограничивается в соответствии с действующим законодательством Российской Федерации (далее - конфиденциальная информация), и наравне с доступностью и целостностью требуется обеспечение конфиденциальности.

Уровень конфиденциальности устанавливается обладателем информации.

3.2. Основными задачами защиты информации в Администрации Молотычевского сельсовета Фатежского района являются:

выявление и оценка потенциальных угроз информационной безопасности и уязвимостей объектов защиты;

исключение либо минимизация выявленных угроз безопасности;

предотвращение инцидентов информационной безопасности.

3.3. Угрозы безопасности информации могут быть реализованы за счет:

- утечки по техническим каналам утечки информации;

- несанкционированного доступа с использованием соответствующего программного обеспечения.

3.4. Угрозы безопасности информации могут проявляться в виде инцидентов информационной безопасности: утрата информации, оборудования или устройств, системные сбои или перегрузки, противоправные и (или) ошибочные действия служащих при работе на АРМ, нарушение правил обработки информации, в том числе разглашение паролей доступа к информационным ресурсам, которые повлекли или могли повлечь нарушение конфиденциальности, целостности и (или) доступности информации, нарушение физических мер защиты, неконтролируемые изменения систем, сбои программного обеспечения, отказы в обслуживании сервисов, средств обработки информации, оборудования, нарушение правил доступа, внедрение вредоносных программ.

В качестве методов защиты информации в Администрации Молотычевского сельсовета Фатежского района применяются: регламентация доступа в служебные помещения, разграничение доступа к техническим средствам и информационным ресурсам, применение антивирусной защиты, применение криптографической защиты информации, применение обезличивания персональных данных, регламентация использования электронной почты, регламентация работы в сети Интернет, регламентация создания и эксплуатации информационных систем, проведение внутреннего контроля и обучение служащих.

IV. Регламентация доступа в служебные помещения Администрации Молотычевского сельсовета Фатежского района

Регламентация доступа в служебные помещения Администрации Молотычевского сельсовета Фатежского 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.

V. Разграничение доступа к техническим средствам и информационным ресурсам Администрации Молотычевского сельсовета Фатежского района

5.1. Разграничение доступа к техническим средствам и информационным ресурсам Администрации Молотычевского сельсовета Фатежского 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.

5.2. Для работы с информационными ресурсами Администрации Молотычевского сельсовета Фатежского района и служащему предоставляется АРМ.

Программное обеспечение (далее - 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.

5.3. К работе с информационными ресурсами Администрации Молотычевского сельсовета Фатежского района допускаются служащие, ознакомленные с настоящей Политикой ИБ.

5.4. Для осуществления доступа к информационным ресурсам Администрации Молотычевского сельсовета Фатежского района служащему создается учетная запись - присваивается уникальный идентификатор (имя, логин) и пароль доступа.

При увольнении учетная запись служащего блокируется.

Обязанность по созданию, блокированию учетных записей возлагается на системных администраторов.

5.5. 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 (на столе, стене, терминале и так далее);

выбирать трудно угадываемый пароль - использовать в пароле строчные и прописные буквы, цифры, специальные символы, не использовать в качестве пароля свои фамилию, имя, отчество, цифровые ряды или повторяющиеся цифры (123456, 111111 и так далее); использовать в пароле не менее 8 символов;

в случае компрометации пароля немедленно изменить пароль.

5.6. При работе на АРМ служащие обязаны: работать только под своей учетной записью; блокировать доступ к АРМ при отсутствии на рабочем месте.

5.7.Служащим запрещается самостоятельно устанавливать на АРМ дополнительные технические средства и (или) ПО.

VI. Антивирусная защита

6.1. Антивирусная защита в Администрации Молотычевского сельсовета Фатежского 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).

6.2. 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.

6.3. Обязанность по установке и регулярному обновлению антивирусного ПО, в том числе антивирусных баз, на АРМ и серверах структурных подразделений Администрации Молотычевского сельсовета Фатежского района и возлагается на соответствующих системных администраторов.

6.4. При установке антивирусного ПО системным администратором должны выполняться следующие требования:

актуализация антивирусных баз на АРМ, подключенных к локальной сети Администрации Молотычевского сельсовета Фатежского района , должна осуществляться ежедневно в автоматическом режиме через специальный сервер обновлений;

актуализация антивирусных баз на АРМ, не подключенных к локальной сети Администрации Молотычевского сельсовета Фатежского района , должна осуществляться с использованием съемных носителей информации не реже одного раза в неделю;

проверка критических областей АРМ, заражение которых вирусами может привести к серьезным последствиям, должна проводиться автоматически при каждой его загрузке.

Некоторые признаки проявления вируса: прекращение работы или неправильная работа ранее успешно функционировавшего ПО, медленная работа АРМ, невозможность загрузки операционной системы, нетипичная работа ПО, вывод на экран непредусмотренных сообщений или изображений, подача непредусмотренных звуковых сигналов, частые зависания и сбои в работе АРМ, частое появление сообщений о системных ошибках.

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

6.5. Служащие допускаются к работе на АРМ только после обучения пользованию средствами антивирусного ПО в соответствии с разделом 12 настоящей Политики ИБ.

VII. Криптографическая защита информации

7.1. Криптографическая защита информации (шифрование) применяется для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении, создания электронной подписи, проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи.

7.2. Применение средств криптографической защиты информации (далее СКЗИ) для шифрования конфиденциальной информации должно осуществляться с учетом требований Приказа Федеральной службы безопасности Российской Федерации от 09.02.2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

7.3. Необходимость криптографической защиты информации конфиденциального характера при ее обработке в информационной системе, выбор применяемых СКЗИ устанавливаются в зависимости от класса информационной системы в соответствии с правовым актом Фатежского района, определяющим порядок эксплуатации информационной системы.

7.4. Шифрование осуществляется перед отправкой данных по незащищенным каналам связи или перед помещением на хранение в ненадежных хранилищах.

7.5. Электронная подпись в Администрации Молотычевского сельсовета Фатежского района используется:

при совершении уполномоченными служащими юридически значимых действий в случаях, установленных действующим законодательством Российской Федерации;

для ведения электронного документооборота, информация которого не относится к информации конфиденциального характера, в соответствии с порядком эксплуатации используемой системы электронного документооборота.

7.6. Электронная подпись выдается аккредитованным удостоверяющим центром служащим, уполномоченным обращаться за получением квалифицированного сертификата (далее - владелец сертификата ключа проверки электронной подписи), в порядке, установленном Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» и регламентом аккредитованного удостоверяющего центра.

7.7. Для хранения сертификата ключа проверки электронной подписи в форме электронного документа (далее - ключевая информация) владельцу сертификата ключа проверки электронной подписи выдается съемный носитель информации (далее - носитель ключевой информации).

7.8. Владелец сертификата ключа проверки электронной подписи обязан: обеспечить безопасное хранение носителя ключевой информации, исключающее бесконтрольный (несанкционированный) доступ к нему неуполномоченных лиц, а также непреднамеренное уничтожение носителя ключевой информации и (или) ключевой информации, хранящейся на нем;

защищать паролем ключевую информацию, хранящуюся на носителе ключевой информации;

подсоединять носитель ключевой информации к АРМ только для подписания электронных документов и в обязательном порядке извлекать из АРМ сразу после окончания работы с ним;

соблюдать конфиденциальность ключевой информации, принимать меры для предотвращения утраты, раскрытия, искажения и несанкционированного использования ключевой информации;

применять для формирования электронной подписи только действующий личный ключ электронной подписи.

7.9. Владельцу сертификата ключа проверки электронной подписи запрещается: отвечать на подозрительные письма с просьбой выслать ключ электронной подписи, пароль или другую конфиденциальную информацию, оставлять носители ключевой информации включенными в АРМ, в легкодоступных местах, в том числе на рабочих столах, знакомить или передавать носители ключевой информации лицам, к ним не допущенным, снимать несанкционированные копии ключевой информации, выводить ключи электронной подписи на дисплей или принтер, записывать на носители ключевой информации с ключами электронной подписи иную (постороннюю) информацию, в том числе рабочую.

7.10. При компрометации ключа электронной подписи - утрате доверия к тому, что используемый ключ электронной подписи обеспечивает безопасность информации, связанной с утерей (в том числе с последующим обнаружением), выходом из строя носителя ключевой информации, нарушением правил хранения, возникновением подозрений на утечку или искажение ключевой информации, владелец сертификата ключа проверки электронной подписи обязан: немедленно прекратить использование ключа электронной подписи при обмене электронными документами с другими пользователями, направить в установленном регламентом аккредитованного удостоверяющего центра порядке заявление об аннулировании сертификата ключа проверки электронной подписи, известить о факте утери (выходе из строя) ключа электронной подписи ответственного за выдачу носителей ключевой информации.

7.11. При увольнении или длительном отпуске владелец сертификата ключа проверки электронной подписи обязан: сдать ключевой носитель, направить в установленном регламентом аккредитованного удостоверяющего центра порядке заявление об аннулировании сертификата ключа проверки электронной подписи.

7.12. Ответственный за выдачу носителей ключевой информации обязан: вести учет носителей ключевой информации, уничтожать в установленном порядке вышедшие из строя носители ключевой информации, убедиться в отсутствии информации на носителе ключевой информации перед его выдачей (Приложение 1).

VIII. Обезличивание персональных данных

8.1. Обезличивание персональных данных в Администрации Молотычевского сельсовета Фатежского 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.

8.2. Обезличивание персональных данных должно осуществляться с учетом требований и методов, утвержденных Приказом Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

8.3. Необходимость и метод обезличивания персональных данных, обрабатываемых в информационной системе персональных данных (далее - ИСПДн), устанавливаются правовым актом Администрации Молотычевского сельсовета Фатежского района, определяющим порядок эксплуатации ИСПДн.

8.4. При использовании процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.

8.5. Обезличивание персональных данных должно производиться перед внесением их в открытую информационную систему и (или) передачей по незащищенным каналам связи.

IX. Регламентация использования электронной почты

9.1. Система электронной почты Администрации Молотычевского сельсовета Фатежского района (далее - электронная почта) используется в информационных целях, в том числе оповещения, организации работы, обеспечения внутренних и внешних коммуникаций.

9.2. Система электронной почты Администрации Молотычевского сельсовета Фатежского района (далее - электронная почта) используется в информационных целях, в том числе оповещения, организации работы, обеспечения внутренних и внешних коммуникаций.

9.3. Система электронной почты Администрации Молотычевского сельсовета Фатежского района (далее - электронная почта) используется в информационных целях, в том числе оповещения, организации работы, обеспечения внутренних и внешних коммуникаций.

9.4. Регламентация использования электронной почты осуществляется с целью снижения риска умышленной или неумышленной несанкционированной рассылки информации, заражения информационных ресурсов Администрации Молотычевского сельсовета Фатежского района вирусами.

9.5. Угрозы, связанные с электронной почтой: возможность создания писем с фальшивыми адресами, возможность нарушения конфиденциальности электронных писем, возможность изменения в процессе передачи содержимого электронных писем, осуществление сетевых атак посредством отправки упакованного в архив сообщения, распаковка которого приводит к выводу системы из строя, заражению вирусами, получение спама.

9.6. Отправка, получение официальных запросов и ответов в целях исполнения своих функций структурными подразделениями Администрации Молотычевского сельсовета Фатежского района осуществляется с использованием официальных адресов электронной почты структурных подразделений Администрации Молотычевского сельсовета Фатежского района.

9.7. Руководитель структурного подразделения Администрации Молотычевского сельсовета Фатежского района определяет специалистов, ответственных за работу с официальной электронной почтой функционального органа, структурного подразделения Администрации Молотычевского сельсовета Фатежского района.

9.8. Отправка, получение электронных сообщений в целях исполнения должностных обязанностей служащими осуществляется с использованием индивидуального электронного адреса служащего в домене ac1te1oyo.ги. При увольнении служащего электронный почтовый ящик отключается с последующим автоматическим удалением.

9.9. При работе с электронной почтой служащие обязаны: перед отправкой тщательно проверять сообщения на отсутствие информации, указанной в пункте 9.6 настоящей Политики ИБ, 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.

9.10. При работе с электронной почтой служащим запрещено:

отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО, разрешенным к использованию в Администрации Молотычевского сельсовета Фатежского района;

отправлять персональные данные без предварительного обезличивания или шифрования;

отправлять сообщения с иного электронного почтового ящика или от имени другого служащего без предоставления полномочий;

использовать электронную почту для создания, отправки, пересылки или хранения любых подрывных, оскорбительных, неэтичных, незаконных материалов, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возраста, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений, национального происхождения, гиперссылок или других ссылок на веб-сайты, содержащие указанные материалы, массовые рассылки спама; рассылать компьютерные коды, файлы или ПО, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования, вирусы или другое злонамеренное ПО, программы для осуществления несанкционированного доступа, серийные номера к программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети Интернет, ссылки на указанную информацию;

перехватывать, изменять, удалять, сохранять или публиковать сообщения иных служащих, кроме случаев, санкционированных руководителями, или в целях администрирования систем;

использовать веб-сервисы Ooo§1e, ОшаИ, НойпаП, УаНоо, Яндекс или подобные почтовые системы третьих сторон («вебмайл») для отправки и (или) получения служебной корреспонденции;

загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным ПО, переходить по активным ссылкам, полученным от отправителей, если имеются сомнения в надежности отправителя и (или) полученного сообщения.

9.11. Содержимое электронного почтового ящика служащего может быть проверено системным администратором без предварительного уведомления служащего в случае подозрения на осуществление рассылки писем, содержащих вредоносное ПО, спам, информацию, распространение которой запрещено правовыми актами. Информация о выявленных нарушениях направляется служащему и руководителю соответствующего структурного подразделения Администрации Молотычевскогосельсовета Фатежского района Курской области.

IX.Регламентация работы в сети Интернет

10.1. Сеть Интернет в Администрации Молотычевского сельсовета Фатежского района используется служащими для получения информации в рамках исполнения должностных обязанностей.

10.2. Регламентация работы в сети Интернет осуществляется с целью снижения риска заражения информационных ресурсов Администрации Молотычевского сельсовета Фатежского района вирусами.

10.3. Организацию доступа к сети Интернет для нужд Администрации Молотычевского сельсовета Фатежского района осуществляет ОВП.

10.4. Доступ к сети Интернет предоставляется служащим с АРМ, закрепленного за служащим для исполнения должностных обязанностей, с использованием учетной записи служащего.

10.5. Угрозы, связанные с работой в сети Интернет:

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

заражение вирусами.

10.6. Служащим запрещается:

осуществлять действия, запрещенные законодательством Российской Федерации;

отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО, разрешенным к использованию в Администрации Молотычевского сельсовета Фатежского района;

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;

передавать информацию, обрабатываемую в Администрации Молотычевского сельсовета Фатежского района, посредством иностранных интернет-сервисов, в том числе систем обмена мгновенными сообщениями, голосовой и видеоинформацией (1С<3, <31Р, 1аЬЬег, У1Ьег, АУйа^{Л}зАрр, 8куре и другие), социальных сетей (ТшШег, ЕасеЬоок,

Ыуе1оита1 и другие), облачных сервисов (1С1оис1, (Эоод1е Ииуе, БгорЬох и другие).

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

10.8. Вся информация об информационных ресурсах, посещаемых служащим, автоматически протоколируется и при необходимости представляется системными администраторами руководителю аппарата Администрации Молотычевского сельсовета Фатежского района, соответствующему руководителю функционального органа, структурного подразделения Администрации Молотычевского сельсовета Фатежского района.

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

X. Регламентация создания, эксплуатации и прекращения эксплуатации информационных систем

11.1. Регламентация создания, эксплуатации и прекращения эксплуатации информационных систем направлена на упорядочение деятельности функциональных органов, структурных подразделений Администрации Молотычевского сельсовета Фатежского района по созданию информационных систем и обеспечению безопасности информации, содержащейся в информационных системах.

11.2. Принятие решения о создании информационной системы или решения о прекращении эксплуатации информационной системы.

11.2.1. Принятие решения о создании информационной системы. Руководитель структурного Администрации Молотычевского сельсовета Фатежского района направляет предложение о создании информационной системы посредством системы электронного документооборота председателю Совета по информационным технологиям при Администрации Молотычевского сельсовета Фатежского района (далее - Совет по ИТ).

Предложение о создании информационной системы должно содержать: обоснование необходимости создания информационной системы, в том числе требования законодательства Российской Федерации, иных правовых актов;

оценку (технико-экономической, социальной и другой) целесообразности создания информационной системы;

цели и задачи информационной системы;

категорию доступа обрабатываемой информации (общедоступная, конфиденциальная);

оператора информационной системы.

Рассмотрение Советом по ИТ предложения о создании информационной системы, порядок принятия Советом по ИТ решения осуществляется в

соответствии с Положением о Совете по информационным технологиям при Администрации Молотычевского сельсовета Фатежского района.

Совет по ИТ принимает решение о целесообразности (об отсутствии целесообразности) создания информационной системы (далее — решение Совета по ИТ), которое оформляется протоколом.

Протокол предоставляется Главе Администрации Молотычевског осельсовета Фатежского района в течение 5 рабочих дней с даты его подписания.

Глава Администрации Молотычевского сельсовета Фатежского района принимает решение о создании информационной системы с учетом решения Совета по ИТ.

11.2.2. Принятие решения о прекращении эксплуатации информационной системы.

Руководитель структурного подразделения Администрации Молотычевского сельсовета Фатежского района направляет посредством системы электронного документооборота Главе Администрации Молотычевского сельсовета Фатежского района предложение о прекращении эксплуатации информационной системы. Предложение о прекращении эксплуатации информационной системы предварительно согласовывается с заместителем главы Администрации Молотычевского сельсовета Фатежского района, осуществляющим оперативное руководство по направлению деятельности.

Предложение о прекращении эксплуатации информационной системы должно содержать:

обоснование необходимости прекращения эксплуатации информационной системы, в том числе ссылки на изменение законодательства Российской Федерации, иных правовых актов, на основании которых функционировала информационная система;

предложения по архивированию, дальнейшему хранению, и (или) уничтожению (стиранию) информации, содержащейся в информационной системе, машинных носителей информации, используемых при эксплуатации информационной системы.

Глава Администрации Молотычевского сельсовета Фатежского района принимает решение о прекращении эксплуатации информационной системы.

11.2.3. Решение о создании информационной системы или решение о прекращении эксплуатации информационной системы утверждается правовым актом Администрации Молотычевского сельсовета Фатежского района. Проект правового акта

Администрации Молотычевского сельсовета Фатежского района подготавливает оператор информационной системы.

11. 2.4. Финансирование работ (услуг) по созданию информационной системы осуществляется за счет бюджета Администрации Молотычевского сельсовета Фатежского района на основании правового акта Администрации Молотычевского сельсовета Фатежского района о создании информационной системы и муниципального контракта на оказание услуг по созданию информационной системы, заключенного в соответствии с требованиями Федерального закона от 05.04.2013 г. № 44- ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

11.3. Процесс создания информационной системы осуществляется в соответствии с ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы стадии создания, утвержденным Постановлением Госстандарта СССР от 29.12.1990 г. № 3469, и представляет собой совокупность упорядоченных во времени, взаимосвязанных, объединенных в стадии и этапы работ, выполнение которых необходимо и достаточно для создания информационной системы.

11.4. Информационная система вводится в эксплуатацию правовым актом Администрации Молотычевского сельсовета Фатежского района. Правовой акт о вводе в эксплуатацию информационной системы должен определять порядок эксплуатации информационной системы.

11.5. Порядок эксплуатации информационной системы должен содержать:

полное наименование информационной системы;

цель создания информационной системы;

законы и иные правовые акты, на основании которых ведется обработка информации в информационной системе и (или) эксплуатация информационной системы;

полномочия структурного подразделения Администрации Молотычевского сельсовета Фатежского района, реализуемые при эксплуатации информационной системы, и (или) задачи, решаемые в информационной системе;

отнесение информационной системы к категории муниципальной или иной в соответствии с требованиями Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

перечень обрабатываемой информации, в том числе персональных данных (при наличии), перечень разделов (для сайтов);

требования по обеспечению безопасности обрабатываемой

информации (конфиденциальности, целостности, доступности);

наименование оператора информационной системы, его права и обязанности;

перечень участников, пользователей информационной системы, их права и обязанности;

порядок обеспечения доступа к информационной системе; иную информацию, определяющую особенности эксплуатации информационной системы.

11.6. Все функционирующие в структурных подразделениях Администрации Молотычевского сельсовета Фатежского района информационные системы включаются в Реестр информационных систем Администрации Молотычевского сельсовета Фатежского района, утвержденный постановлением Администрации Молотычевского сельсовета Фатежского района (далее - Реестр информационных систем).

Основанием для включения информационной системы в Реестр информационных систем является правовой акт Администрации Молотычевского сельсовета Фатежского района о вводе в эксплуатацию информационной системы.

11.7. Основанием для изменения информации об информационной системе, включенной в Реестр информационных систем, является правовой акт Администрации Молотычевского сельсовета Фатежского района, определяющий порядок эксплуатации информационной системы.

11.8. Основанием для исключения информационной системы из Реестра информационных систем является правовой акт Администрации Молотычевского сельсовета Фатежского района о прекращении эксплуатации информационной системы.

XI. Проведение внутреннего контроля и обучение служащих

12.1. В целях выявления угроз безопасности информации, нарушений настоящей Политики ИБ и принятия мер, направленных на предотвращение угроз и нарушений, в Администрации Молотычевского сельсовета Фатежского района осуществляется внутренний контроль:

12.1.1. использования технических средств, ПО, работы в сети Интернет в структурных подразделениях Администрации Молотычевского сельсовета Фатежского района по поручению руководителей структурных подразделений Администрации Молотычевского сельсовета Фатежского района.

12.1.2. обработки персональных данных в Администрации Молотычевского сельсовета Фатежского района в соответствии с утвержденными требованиями к защите персональных

данных, установленным Федеральным законом «О персональных данных».

12.2. Ознакомление служащих с настоящей Политикой ИБ производится при: приеме на работу, изменении настоящей Политики ИБ, обнаружении действий служащих, которые повлекли или могли повлечь нарушение безопасности информации.

12.3. Обучение служащих пользованию средствами антивирусного ПО производится при: приеме на работу, изменении антивирусного ПО, заражении АРМ вирусами.

12.4. Обязанность по организации ознакомления служащих с настоящей Политикой ИБ возлагается на руководителей структурных подразделений Администрации Молотычевского сельсовета Фатежского района. Обязанность по обучению пользованию средствами антивирусного ПО возлагается на системных администраторов.

XII. Ответственность за нарушения настоящей Политики ИБ

13.1. Служащие в рамках должностных обязанностей и полномочий несут ответственность в соответствии с действующим законодательством Российской Федерации за:

невыполнение требований настоящей Политики ИБ; действия или бездействие, ведущие к нарушению информационной безопасности;

действия или бездействие, ведущие к нарушению действующего законодательства Российской Федерации в области информационных технологий.

13.2. При обнаружении нарушения служащими настоящей Политики ИБ системный администратор устанавливает причины возникновения нарушения и направляет служебную записку о выявленном нарушении руководителю структурного подразделения Администрации Молотычевскогосельсовета Фатежского района Курской области.

Руководитель структурного подразделения Администрации Молотычевского сельсовета Фатежского района принимает решение о необходимости привлечения служащего к ответственности.

Системный администратор ведет учет всех выявленных случаев нарушения безопасности информации.

Приложение 1

РУКОВОДСТВО по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

(разработано во исполнение пункта 1 части 2 статьи 13 и части 4 статьи 18 Федерального закона от 06.04.2011 г. № 63-ФЗ «Об электронной подписи»)

1. Общие положения

Настоящее руководство составлено в соответствии с требованиями Федерального закона от 0 6 . 0 4 . 2 0 1 1 г. № 63-ФЗ «Об электронной подписи» и является средством официального информирования лиц, владеющих квалифицированной электронной подписью, об условиях, рисках и порядке использования квалифицированной электронной подписи и средств электронной подписи, а также о мерах, необходимых для обеспечения безопасности при использовании квалифицированной электронной подписи.

При применении квалифицированной электронной подписи в информационных системах владельцу сертификата необходимо выполнять требования:

Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 г. № 152, в части обращения со средствами криптографической защиты информации;

Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом Федеральной службы безопасности Российской Федерации от 09.02.2005 г. № 66, в части эксплуатации средств криптографической защиты информации;

эксплуатационной документации к средствам электронной подписи;

приведенных ниже организационно-технических и административных мер по обеспечению правильного функционирования средств обработки и передачи информации.

2. Требования по размещению

При размещении средств вычислительной техники с установленными на них средствами квалифицированной электронной подписи:

должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены средства квалифицированной электронной подписи, посторонним лицам, не имеющим допуск к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями во избежание негативных воздействий с их стороны на средства электронной подписи, средства криптографической защиты и передаваемую информацию;

- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

3. Требования по установке средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

3.1. При использовании средств квалифицированной электронной подписи должны выполняться следующие меры по защите информации от несанкционированного доступа:

- Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т. д.), использовать фильтры паролей в соответствии со следующими правилами: длина пароля должна быть не менее 6 символов, в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т. п.), пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т. д.), а также сокращения (USER, ADMIN, root, и т. д.), при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях, личный пароль пользователь не имеет права никому сообщать, периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 календарных дней.

При использовании ключей электронных подписей средства вычислительной техники должны быть сконфигурированы с учетом следующих требований: не использовать нестандартные, измененные или отладочные версии операционных систем, исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой, исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек, на средствах вычислительной техники с установленными

средствами квалифицированной электронной подписи должна быть установлена только одна операционная система, все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т. п.), режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень, всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права, необходимо предусмотреть меры, максимально ограничивающие доступ к: системному реестру, файлам и каталогам, временным файлам, журналам системы, файлам подкачки, кэшируемой информации (пароли и т. п.), отладочной информации.

3.1.2. На средствах вычислительной техники необходимо:

организовать удаление (по окончании сеанса работы средств квалифицированной электронной подписи) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их работы. Если это невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;

исключить попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий;

регулярно устанавливать пакеты обновлений безопасности операционной системы (Service Packs, Hot fix и т.п.), обновлять антивирусные базы.

3.1.3. В случае подключения технических средств с установленными средствами квалифицированной электронной подписи к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

Необходимо организовать и использовать: систему аудита, организовать регулярный анализ результатов аудита, комплекс мероприятий по антивирусной защите.

Запрещается: осуществлять несанкционированное копирование ключевых носителей, разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер и иные средства отображения информации, использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя, вносить какие-либо изменения в программное обеспечение средств квалифицированной электронной подписи, записывать на ключевые носители постороннюю информацию, оставлять средства вычислительной техники с установленными средствами квалифицированной электронной подписи без контроля после ввода ключевой информации, использовать ключ электронной подписи и соответствующий сертификат ключа проверки электронной подписи, Заявление на изменение статуса которого подано в территориальный орган Федерального казначейства, в течение времени, исчисляемого с момента подачи Заявления на изменение статуса сертификата по момент официального информирования об изменении статуса сертификата, либо об отказе в изменении статуса, использовать ключ электронной подписи, связанный с сертификатом

ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено, удалять ключевую информацию с ключевого носителя до истечения срока действия, аннулирования или прекращения действия сертификата ключа проверки электронной подписи.

4. Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации, содержащими ключи квалифицированной электронной подписи

4.1. Меры защиты ключей квалифицированной электронной подписи.

Ключи квалифицированной электронной подписи при их создании должны записываться на предварительно проинициализированные (отформатированные) ключевые носители, типы которых поддерживаются используемым средством квалифицированной электронной подписи согласно технической и эксплуатационной документации к ним.

Ключевые носители должны иметь маркировку с учетным номером, присвоенным Заявителем.

Ключи квалифицированной электронной подписи на ключевом носителе могут быть защищены паролем (ПИН-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство квалифицированной электронной подписи.

Ответственность за конфиденциальность сохранения пароля (ПИН- кода) возлагается на владельца ключа квалифицированной электронной подписи.

4.2. Обращение с ключевой информацией и ключевыми носителями.

Недопустимо пересылать файлы с ключевой информацией для работы в информационных системах по электронной почте сети Интернет или по внутренней электронной почте (кроме открытых ключей).

Размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами квалифицированной электронной подписи, способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками.

Носители ключевой информации должны использоваться только их владельцем и храниться в месте не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т. д.).

Носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средствами квалифицированной электронной подписи операций формирования и проверки квалифицированной электронной подписи, шифрования и дешифрования. Размещение носителя ключевой информации в

считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

На носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

4.3. Обеспечение безопасности АРМ с установленными средствами квалифицированной электронной подписи.

С целью контроля исходящего и входящего подозрительного трафика, технические средства с установленными средствами квалифицированной электронной подписи должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования. На технических средствах, используемых для работы в информационных системах: на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие требованиям, приведенным в разделе 3, должно быть установлено только лицензионное программное обеспечение, должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных, должны быть отключены все неиспользуемые службы и процессы операционной системы Windows (в т. ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски и т. д.), должны регулярно устанавливаться обновления операционной системы, должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами квалифицированной электронной подписи и средствами криптографической защиты третьих лиц, не имеющих полномочий для работы в соответствующей информационной системе, должна быть активирована регистрация событий информационной безопасности, должна быть включена автоматическая блокировка экрана после ухода ответственного сотрудника с рабочего места.

В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства квалифицированной электронной подписи, необходимо гарантированно удалить всю информацию (при условии исправности технических средств), использование которой третьими лицами может потенциально нанести вред организации, в том числе средства квалифицированной электронной подписи, журналы работы систем обмена электронными документами и так далее.