АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОКРУГА МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ КРАСНОДОНСКИЙ МУНИЦИПАЛЬНЫЙ ОКРУГ ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ

ПОСТАНОВЛЕНИЕ

«30» мая 2024 г. № 210

г. Краснодон

Об утверждении Политики информационной безопасности Администрации муниципального округа муниципальное образование Краснодонский муниципальный округ Луганской Народной Республики

В соответствии с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», руководствуясь Уставом муниципального образования Краснодонский муниципальный округ Луганской Народной Республики, принятым решением Совета муниципального округа муниципальное образование Краснодонский муниципальный округ Луганской Народной Республики от 30 октября 2023 года № 1, с целью обеспечения информационной безопасности Администрация муниципального округа муниципальное образование Краснодонский муниципальный округ Луганской Народной Республики

ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемую Политику информационной безопасности Администрации муниципального округа муниципальное образование Краснодонский муниципальный округ Луганской Народной Республики.
2. Определить структурным подразделением, осуществляющим функции по обеспечению информационной безопасности, управление внутренней политики Администрации муниципального округа муниципальное образование Краснодонский муниципальный округ Луганской Народной Республики.
3. Настоящее постановление вступает в силу со дня его подписания и подлежит опубликованию на официальном сайте муниципального образования Краснодонский муниципальный округ Луганской Народной Республики в

информационно-телекоммуникационной сети «Интернет» (http://krasnodon-adm.ru/).

4. Контроль за исполнением настоящего постановления возложить на заместителя Главы Администрации муниципального округа муниципальное образование Краснодонский муниципальный округ Луганской Народной Республики Галушкину Т.А.

Глава муниципального округа
муниципальное образование
Краснодонский муниципальный округ
Луганской Народной Республики С.П. Козенко

УТВЕРЖДЕНА
постановлением Администрации
муниципального округа
муниципальное образование
Краснодонский муниципальный округ
Луганской Народной Республики
от «30» мая 2024 г. № 210

Политика информационной безопасности Администрации муниципального округа муниципальное образование Краснодонский муниципальный округ Луганской Народной Республики

I. Общие положения

1.1. Настоящая Политика информационной безопасности Администрации муниципального округа муниципальное образование Краснодонский муниципальный округ Луганской Народной Республики (далее - Политика ИБ) разработана в целях установления безопасных способов обработки информации в электронном виде, в том числе в информационных системах (сайтах) Администрации Муниципального округа муниципальное образование Краснодонский муниципальный округ Луганской Народной Республики (далее - информационная система).

1.2. Настоящая Политика ИБ определяет в Администрации муниципального округа муниципальное образование Краснодонский муниципальный округ Луганской Народной Республики (далее – Администрация) цели и задачи защиты информации, устанавливает методы защиты информации, которыми должны руководствоваться муниципальные служащие Администрации, иные работники Администрации, 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, 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. При осуществлении санкционированного доступа к информационным ресурсам Администрации 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 - функциональный орган или структурное подразделение Администрации, 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;

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». 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, основные виды угроз безопасности информации

3.1. Обеспечение информационной безопасности в Администрации (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 является вся информация, обрабатываемая в Администрации (структурных подразделениях) (далее - информация), независимо от ее местонахождения в информационной среде.

В Администрации 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 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 возникнуть за счет:

- утечки информации по техническим каналам;

- 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 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.

IV. Регламентация доступа в служебные помещения Администрации

4.1. Регламентация доступа в служебные помещения Администрации 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

5.1. Разграничение доступа к техническим средствам и информационным ресурсам Администрации 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 служащему предоставляется АРМ. Программное обеспечение (далее - ПО) АРМ устанавливается и обновляется системным администратором со специальных ресурсов или съемных носителей в соответствии с лицензионным соглашением.

5.3. 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.

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

VI. Антивирусная защита

6.1. Антивирусная защита в Администрации 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.

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. Электронная подпись в Администрации 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.

7.4. 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.

7.5. 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).

7.6. 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.

7.7. 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.

7.8. 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.

7.9. При увольнении 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.

7.10. 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 в соответствии с Руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (Приложение).

VIII. Регламентация использования электронной почты

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

8.2. Регламентация использования электронной почты осуществляется с целью снижения риска умышленной или неумышленной несанкционированной рассылки информации, заражения информационных ресурсов Администрации вирусами.

8.3. 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.

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

8.5. Руководитель структурного подразделения Администрации определяет специалистов, ответственных за работу с официальной электронной почтой функционального органа, структурного подразделения Администрации.

8.6. 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.

8.7. При работе с электронной почтой служащим запрещено: отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО, разрешенным к использованию в Администрации; 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.

8.8. 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.

IX. Регламентация работы в сети Интернет

9.1. Сеть Интернет в Администрации служащими для получения информации в рамках исполнения должностных обязанностей.

9.2. Регламентация работы в сети Интернет осуществляется с целью снижения риска заражения информационных ресурсов Администрации вирусами.

9.3. Организацию доступа к сети Интернет для нужд Администрации осуществляет ОВП.

9.4. Доступ к сети Интернет предоставляется служащим с АРМ.

9.5. Угрозы, связанные с работой в сети Интернет:

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

заражение вирусами.

9.6. Служащим запрещается:

осуществлять действия, запрещенные законодательством Российской Федерации и Луганской Народной Республики;

отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО, разрешенным к использованию в Администрации;

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, посредством иностранных интернет-сервисов, в том числе систем обмена мгновенными сообщениями, голосовой и видеоинформацией (Viber, WhatsApp, Skype и другие), социальных сетей (Facebook, Instagram, Twitter, LiveJournal и другие).

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

X. Проведение внутреннего контроля и обучение служащих

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

10.1.1. использования технических средств, ПО, работы в сети Интернет в структурных подразделениях Администрации.

10.1.2. обработки персональных данных в Администрации в соответствии с утвержденными требованиями к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

XI. Ответственность за нарушения настоящей Политики ИБ

11.1. 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.

Приложение
к Политике информационной
безопасности Администрации
муниципального округа
муниципальное образование
Краснодонский муниципальный округ
Луганской Народной Республики

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 06.04.2011 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 обеспечению информационной безопасности при обращении с носителями ключевой информации, содержащими ключи квалифицированной электронной подписи

2.1. 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.

2.2. 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).