

**Муниципальное бюджетное дошкольное образовательное учреждение
детский сад №39 муниципального образования Темрюкский район**

Утверждаю
Заведующий МБДОУ ДС №39
_____ О.И. Салихова
Приказ № _____ от _____ г.

**ИНСТРУКЦИЯ
ПО ПОРЯДКУ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ПОМОЩИ КРИПТОСРЕДСТВ**

1. Общая часть

1.1. Настоящие функциональные обязанности разработаны в соответствии с приказом ФАПСИ от 13.06.2001 г. №152 «Об утверждении 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».

1.2. Ответственный пользователь средств криптографической защиты информации (далее - СКЗИ), назначается из числа сотрудников ОРГАНИЗАЦИЯ и освобождается от этих обязанностей приказом руководства ОРГАНИЗАЦИЯ.

2. Квалификационные требования

Профессиональные знания и навыки:

2.1. Ответственный пользователь СКЗИ в своей работе руководствуется следующими нормативными документами:

- «Инструкцией 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 ФАПСИ от 13 июня 2001 года № 152;
- приказом ФСБ России от 9 февраля 2005 года №66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- приказом ФСБ от 10 июля 2014 года №378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

– «Методическими рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденными руководством 8 Центра ФСБ России (№149/7/2/6-432 от 31.03.2015);

– инструкциями к СКЗИ и иными организационно-распорядительными документами.

3. Функциональные обязанности

В обязанности ответственного пользователя СКЗИ входит:

3.1. Своевременное и качественное исполнение поручений руководства ОРГАНИЗАЦИЯ, данные в пределах их полномочий, установленных законодательством Российской Федерации.

3.2. Оказание консультационной помощи по вопросам соблюдения защиты информации при обращении со средствами криптографической защиты информации.

3.3. Постоянное повышение профессиональных навыков и умений, необходимых для надлежащего исполнения функциональных обязанностей.

3.4. Знание порядка эксплуатации используемых в ОРГАНИЗАЦИЯ СКЗИ.

3.5. Ведение установленного нормативными документами учета СКЗИ, ключевых документов, сертификатов электронных цифровых подписей.

3.6. Соблюдение режима конфиденциальности при обращении со сведениями, полученными при исполнении функциональных обязанностей, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документах к ним.

3.7. Надежное хранение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

3.8. Выявление попыток посторонних лиц получить сведения о защищаемой конфиденциальной информации, об используемых СКЗИ или ключевых документах к ним и своевременное оповещение об этом руководителя органа криптографической защиты информации.

3.9. Немедленное принятие мер по предупреждению разглашения защищаемых сведений конфиденциального характера, а также возможной утечки таких сведений при выявлении фактов утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

Ответственный пользователь СКЗИ осуществляет следующие функции:

3.10. Осуществляет профилактическую деятельность по соблюдению требований руководящих документов, технической, эксплуатационной документации с сотрудниками ОРГАНИЗАЦИЯ, назначенными пользователями СКЗИ.

3.11. Участвует в проведении служебных расследований по фактам нарушения требований по обращению с СКЗИ.

3.12. Принимает меры к предотвращению разглашения и утечки информации ограниченного доступа при эксплуатации и хранении специальных технических средств, предназначенных для передачи, приема и обработки конфиденциальной информации, а также при использовании незащищенных каналов связи.

3.13. Участвует в разработке методических и нормативных материалов и оказании необходимой методической помощи в проведении работ по защите информации при обращении с СКЗИ.

4. Права

Ответственный пользователь СКЗИ имеет право:

4.1. Осуществлять плановые и внеплановые проверки функционирования СКЗИ, наличия ключевых документов и технической документации с СКЗИ.

4.2. Осуществлять, в рамках своей компетенции, взаимодействие с организациями-производителями СКЗИ.

4.3. При изменении состава СКЗИ получить профессиональную переподготовку, повышение квалификации и стажировку в порядке, установленном законодательством Российской Федерации.

4.4. Ходатайствовать о проведении служебной проверки.

5. Ответственность

Ответственный пользователь СКЗИ несет персональную ответственность в соответствии с законодательством Российской Федерации за:

5.1. Выполнение возложенных на него обязанностей и правильное использование предоставленных ему прав в соответствии с данными функциональными обязанностями.

5.2. Несвоевременное или некачественное выполнение распоряжений руководства ОРГАНИЗАЦИЯ.

5.3. Разглашение сведений, отнесенных к сведениям ограниченного доступа, ставших известными в ходе выполнения функциональных обязанностей или иным путем, утрату их носителей, передачу третьим лицам, публикацию без разрешения руководства, а также использование для занятия любой деятельностью, которая может нанести ущерб.

ПАМЯТКА при работе с шифровальными (криптографическими) средствами

1. К шифровальным (криптографическим) средствам относят:

– средства электронной подписи (ЭП);

- средства шифрования информации на съемных носителях;
- средства шифрования информации, передающейся по каналам связи;
- средства изготовления ключевых документов и носители ключевой информации.

2. Пользователи криптосредств несут персональную ответственность за сохранность криптосредств, ключевой, эксплуатационной и технической документации.

3. Пользователи криптосредств обязаны:

- хранить в тайне информацию, к которой они были допущены, в том числе сведения о криптосредствах, ключевых документах к ним, технической и эксплуатационной документации и других мерах защиты;

- не допускать копирования ключевых документов;

- не допускать записи на ключевой носитель посторонней информации;

- подключать ключевые носители только к устройству, предназначенному для работы с криптосредством;

- передавать персональные данные (далее – ПДн) по внешним каналам связи только с использованием криптосредств;

- соблюдать требования по обеспечению безопасности персональных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним;

- сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;

- делать резервную копию персональных ключей шифрования и сдавать на хранение ответственному за обслуживание шифровальных (криптографических) средств;

- немедленно уведомлять руководителя и ответственного за обработку персональных данных о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых ПДн;

- при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств, сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы ответственному пользователю СКЗИ;

4. Безопасность обработки ПДн с использованием криптосредств обеспечивается:

- соблюдением пользователями криптосредств конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых криптосредств и ключевых документах к ним;

- точным выполнением пользователями криптосредств требований к обеспечению безопасности персональных данных;

- надёжным хранением эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения;

– своевременным выявлением попыток посторонних лиц получить сведения о защищаемых персональных данных, об используемых крипто средствах или ключевых документах к ним;

– немедленным принятием мер по предупреждению разглашения защищаемых персональных данных, а также возможной их утечки при выявлении фактов утраты или недостачи крипто средств, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.