ПРИЛОЖЕНИЕ №22
УТВЕРЖДЕНО
Приказом «О вводе в действие комплекта организационно-распорядительной документации по организации обработки и защиты персональных данных» МБОУ Сокольская СШ
от «30» августа 20 24 г.
№ 595

(М.П.)

Инструкция

пользователя средств криптографической защиты информации

Оглавление

1. Общие положения

1.1. Муниципальное бюджетное общеобразовательное учреждение Сокольская средняя школа (далее – Организация) руководствуется настоящей Инструкцией пользователя средств криптографической защиты информации в Организации (далее - Инструкция), определяющей действия и обязанности работников при обработке персональных данных в информационных системах персональных данных с использованием средств криптографической защиты информации.

1.2. Сокращения, термины и определения:

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	**Расшифровка сокращения**
СКЗИ, криптосредство	Средство криптографической защиты информации

Таблица 2 – Перечень терминов и определений

Термин	**Определение**	**Источник**
Информация	Сведения (сообщения, данные) независимо от формы их представления	ГОСТ Р 50922-2006
Ключевая информация	Специальным образом организованная совокупность криптоключей, предназначенных для осуществления криптографической защиты информации в течение определенного срока	Приказ ФАПСИ от 13.06.2001 № 152
Ключевой документ	Физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и технологическую информацию	Приказ ФАПСИ от 13.06.2001 № 152
Компрометация криптоключей	Хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам	Приказ ФАПСИ от 13.06.2001 № 152
Криптографический ключ (криптоключ)	Совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе	Приказ ФАПСИ от 13.06.2001 № 152
Пользователь СКЗИ	Физическое лицо, непосредственное допущенное к работе с СКЗИ	Приказ ФАПСИ от 13.06.2001 № 152

Термин	Определение	Источник
Спецпомещение	Помещение, где установлены СКЗИ или хранятся ключевые документы к ним	Приказ ФАПСИ от 13.06.2001 № 152
СКЗИ	Шифровальные (криптографические) средства защиты информации конфиденциального характера. К СКЗИ относятся: - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи, включая СКЗИ; - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от несанкционированного доступа к информации при ее обработке и хранении; - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и "электронной подписи"; - аппаратные, программные и аппаратно-программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ независимо от вида носителя ключевой информации.	Приказ ФАПСИ от 13.06.2001 № 152

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

приказ Федерального агентства правительственной связи и информации при Президенте РФ от 13.06.2001 № 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»,

приказ Федеральной службы безопасности Российской Федерации от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005)»,

приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 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 требованиям к защите персональных данных для каждого из уровней защищенности».

1.4. Пользователи криптосредств допускаются к работе с СКЗИ приказом руководителя Организации с последующим обязательным ознакомлением Ответственного пользователя криптосредств.

1.5. Пользователи криптосредств должны быть ознакомлены с настоящей Инструкцией, Положением по использованию средств криптографической защиты информации в Организации под роспись.

2. Обязанности Пользователя криптосредств

2.1. Пользователь криптосредств при эксплуатации СКЗИ, используемых для обеспечения безопасности персональных данных при их обработке в информационной системе персональных данных должен выполнять требования нормативных и правовых актов Российской Федерации, Положения по использованию средств криптографической защиты информации, настоящей Инструкции, эксплуатационной, технической, и организационно-распорядительной документации для информационной системы персональных, в том числе для СКЗИ.

2.2. Пользователь криптосредств обязан:

- пройти обучение правилам работы с СКЗИ и ознакомиться с Положением по использованию средств криптографической защиты информации, Инструкцией пользователя криптосредств и нормативными правовыми актами Российской Федерации, регламентирующими обеспечение безопасности информации с использованием криптосредств.

- получить у Ответственного пользователя криптосредств СКЗИ, эксплуатационную и техническую документацию, ключевые документы с документальным оформлением (под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов);

- получить у Ответственного пользователя криптосредств ключ от металлического хранилища (сейфа) для хранения инсталлирующих СКЗИ носителей, эксплуатационной и технической документации к криптосредствам, ключевых документов с документальным оформлением (под расписку в Журнале учета металлический хранилищ (сейфов));

- хранить инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение. Хранить резервные ключевые

документы, предназначенные для применения в случае компрометации действующих криптоключей, раздельно от действующих ключевых документов;

- вести технический (аппаратный) журнал в случае, если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ. Регистрировать в техническом (аппаратном) журнале разовый ключевой носитель или электронную запись соответствующего криптоключа, а также отражать данные об эксплуатации СКЗИ и другие сведения, предусмотренные эксплуатационной и технической документацией. Самостоятельно уничтожать разовые ключевые носители, электронные записи ключевой информации, соответствующей выведенным из действия криптоключам и делать об этом отметку под расписку в техническом (аппаратном) журнале;

- соблюдать режим конфиденциальности информации, которая стала известной в процессе выполнения должностных обязанностей, в том числе сведений о криптоключах, паролях и применяемых СКЗИ, организации хранения, обработки и передачи связи информации с использованием СКЗИ;

- выполнять требования эксплуатационных и регламентирующих документов по обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных с использованием СКЗИ;

- контролировать целостность печатей (пломб) на системных блоках технических средств с установленными СКЗИ;

- осуществлять уничтожение ключевых документов с документальным оформлением (под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов) после окончания срока действия, не позднее 10 суток после вывода их из действия, если иной срок уничтожения не предусмотрен эксплуатационной и технической документацией к СКЗИ;

- сообщать Ответственному пользователю криптосредств о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

- сдать с документальным оформлением (под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов) СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы Ответственному пользователю криптосредств при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

- сдать с документальным оформлением (под расписку в Журнале учета металлический хранилищ (сейфов)) ключ от металлического хранилища (сейфа) Ответственному пользователю криптосредств при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

- немедленно уведомлять Ответственного пользователя криптосредств и руководителя Организации о фактах утраты или недостачи СКЗИ, ключевых

документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений;

- немедленно выводить из действия криптоключи, в отношении которых возникло подозрение в компрометации, с уведомлением Ответственного пользователя криптосредств и руководителя Организации с последующим их уничтожением.

2.3. Пользователям криптосредств запрещается:

- разглашать информацию о ключевых документах и информацию ограниченного доступа;
- вносить любые изменения в программное обеспечение СКЗИ, изменять настройки СКЗИ;
- допускать к использованию СКЗИ посторонних лиц;
- осуществлять вскрытие системных блоков технических средств с установленными СКЗИ, подключать к ним дополнительные устройства;
- использовать криптоключи, в отношении которых возникло подозрение в компрометации
- оставлять ключевые носители без контроля, выносить их за пределы служебных помещений;
- снимать копии с ключевых документов;
- записывать на ключевой носитель информацию, не предусмотренную правилами пользования СКЗИ (служебные файлы, текстовые и мультимедийные файлы и т.п.);
- допускать установку ключевых документов в другие ПЭВМ;
- выводить ключевую информацию на средствах отображения информации (дисплей монитора, печатающие устройства, проекторы и т.п.).

3. Ответственность

3.1. Пользователь криптосредств несет ответственность за несоблюдение требований документов, регламентирующих организацию и обеспечение функционирования и безопасности СКЗИ, предназначенных для защиты персональных данных при их обработке в информационной системе персональных данных, в соответствии с действующим законодательством Российской Федерации.