Приложение № 8
к политике информационной безопасности
ГБУ ДО СК «Комплексная спортивная школа»

ПОЛОЖЕНИЕ

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. Назначение и область действия.

1.1. Настоящее Положение об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты (далее – СКЗИ) информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (далее – конфиденциальной информации) разработано во исполнение Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»; Приказа ФСБ России от 10.07.2014 N 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»; «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 ФАПСИ от 13 июня 2001 г. №152; «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ - 2005)», утвержденного приказом ФСБ РФ от 9 февраля 2005 г. N 66; эксплуатационной и технической документации на используемые в Учреждении СКЗИ, а также внутренних нормативных документов.

1.2. Настоящее положение определяет основные правила и требования по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации в государственном бюджетном учреждении дополнительного образования Ставропольского края «Комплексная спортивная школа» (далее – учреждение).

1.3. Распространяется на всех работников Учреждения. Является обязательным для исполнения.

2. Основные требования.

2.1 В целях разработки и осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ конфиденциальной информации в Учреждении создана инструкция пользователя средств криптографической защиты информации ГБУ ДО СК «Комплексная спортивная школа» (Приложение 1 к настоящему Положению).

2.2 В целях обеспечения безопасного хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации приказом директора Учреждения назначены пользователи СКЗИ, которые в своей деятельности руководствуются Инструкцией пользователя СКЗИ,

3. Роли и ответственность.

3.1. Ответственность за соблюдение данного Положения возлагается на всех работников учреждения.

3.2. Ответственность за реализацию данного Положения возлагается на руководителей подразделений Учреждения; пользователей СКЗИ и сотрудников сектора криптографической защиты.

Приложение 1.

УТВЕРЖДЕНА

приказом государственного
бюджетного учреждения
дополнительного образования
Ставропольского края «Комплексная
спортивная школа»

от _____2024 г. № _____

ИНСТРУКЦИЯ
пользователя средств криптографической защиты информации ГБУ ДО СК «Комплексная спортивная школа»

1. Общие положения

1.1. Настоящая Инструкция разработана в целях регламентации действий пользователей, допущенных к работе со средствами криптографической защиты информации (СКЗИ) в ГБУ ДО СК «Комплексная спортивная школа» (далее – Организация), которые осуществляют свои должностные обязанности с использованием СКЗИ.

1.2. Под использованием СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов и т.д.

1.3. СКЗИ должны использоваться для защиты конфиденциальной информации (включая персональные данные).

1.4. Настоящая Инструкция в своем составе, терминах и определениях основывается на положениях:

– «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 ФАПСИ от 13 июня 2001 г. №152 (далее – Инструкция ФАПСИ от 13 июня 2001 г. №152);

– Приказа ФСБ России от 10.07.2014 N 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»;

– Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

– ГОСТ Р 59853-2021 Информационные технологии (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

2. Термины и определения

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну.

Исходная ключевая информация – совокупность данных, предназначенных для выработки по определенным правилам криптоключей.

Ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

Ключевой документ – физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию.

Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации).

Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

Криптографический ключ (криптоключ) – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

Орган криптографической защиты (ОКЗ) – организация, структурное подразделение организации - лицензиата ФАПСИ, обладателя конфиденциальной информации. разрабатывающая и осуществляющая мероприятия по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации ограниченного доступа.

Автоматизированное рабочее место (АРМ) - программно-технический комплекс автоматизированной системы, предназначенный для автоматизации

деятельности определенной категории пользователей или определенного вида деятельности.

Пользователи СКЗИ – работники Организации, непосредственно допущенные к работе с СКЗИ.

Средство криптографической защиты информации (СКЗИ) - совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией, и которая используется для определения лица, подписывающего информацию.

3. Порядок получения допуска пользователей к работе с СКЗИ

3.1. Для работы с СКЗИ привлекаются работники, назначенные соответствующим приказом руководителя организации и прошедшие обучение и проверку знаний законодательства РФ, руководящих документов ФАПСИ и ФСБ (радел 1 настоящей инструкции) и локальных актов учреждения по вопросам обеспечения безопасности при работе с шифровальными (криптографическими) средствами защиты информации.

4. Обязанности пользователей СКЗИ

4.1. Пользователи СКЗИ обязаны:

– осуществлять эксплуатацию СКЗИ в соответствии с документацией на СКЗИ, а также в соответствии с иными нормативными правовыми актами, регулирующими отношения в области обеспечения безопасности при работе с шифровальными (криптографическими) средствами защиты информации, в том числе настоящей Инструкцией;

– не разглашать конфиденциальную информацию, к которой они допущены, в том числе сведения о используемых СКЗИ или ключевых документах к ним;

– соблюдать требования к обеспечению безопасности конфиденциальной информации, обрабатываемой с использованием СКЗИ;

– сообщать в орган криптографической защиты (далее – ОКЗ) о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

– сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

– немедленно уведомлять ответственного пользователя СКЗИ или сотрудников ОКЗ 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;

– прекратить работу с СКЗИ при обнаружении на автоматизированном рабочем месте (далее – АРМ), оборудованном СКЗИ, посторонних программ или вирусов. Незамедлительно организовать мероприятия по анализу и ликвидации негативных последствий данного нарушения;

– хранить инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в запираемых шкафах (ящиках, хранилищах), исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение;

– при отсутствии запирающегося хранилища ключевые документы помещаются в тубус, опечатываются личной печатью (при отсутствии личной печати тубус опечатывается печатями сотрудников ОКЗ № 30, 31 или 7) и передается руководителю структурного подразделения, который помещает тубус в личный сейф по окончанию рабочего дня;

– получать вновь изготовленные ключевые документы, эксплуатационную и техническую документацию к ним у сотрудников ОКЗ с росписью в «журнале выдачи ключевых документов»;

– передавать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы только между пользователями СКЗИ и (или) сотрудниками ОКЗ под расписку в соответствующих журналах поэкземплярного учета.

4.2.Не допускается:

– разглашать конфиденциальную информацию, к которой был допущен Пользователь СКЗИ;

– разглашать содержимое ключевых носителей или передавать сами носители лицам, к ним не допущенным;

– осуществлять несанкционированное копирование ключевых носителей;

– использовать ключевой носитель при проведении работ, не являющихся штатными процедурами использования ключей электронной подписи (далее – ЭП) (шифрование/расшифровывание информации,

проверка ЭП и т.д.), а также вставлять ключевой носитель в порты других компьютеров;

– записывать на ключевом носителе постороннюю информацию;

– оставлять ключевые носители с ключевой документацией без присмотра;

– вносить какие-либо изменения в программное обеспечение СКЗИ;

– использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей).

4.3. О нарушениях, которые могут привести к компрометации ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей или передававшейся (хранящейся) с их использованием конфиденциальной информацией, пользователи СКЗИ обязаны сообщать в ОКЗ или ответственному пользователю СКЗИ.

5. Ответственность пользователей СКЗИ

5.1. Пользователи СКЗИ отвечают за сохранность конфиденциальной информации, которая стала ему известной вследствие исполнения им своих служебных обязанностей.

5.2. Пользователи СКЗИ несут персональную ответственность за сохранность полученных экземпляров СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

5.3. Ответственность лиц, допущенных к работе с СКЗИ, за неисполнение и/или ненадлежащее исполнение своих обязанностей, предусмотренных соответствующими инструкциями, а также за разглашение конфиденциальной информации, ставшей ему известной вследствие исполнения им своих служебных обязанностей, определяется действующим законодательством Российской Федерации и условиями трудового договора.

5.4. На АРМ, оборудованном СКЗИ, программное обеспечение должно быть лицензионным. Пользователь несет ответственность за то, чтобы на АРМ, на котором установлены СКЗИ, не были установлены и не эксплуатировались программы (в том числе, программы-вирусы), которые могут нарушить функционирование СКЗИ.