ИНСТРУКЦИЯ

пользователя по обращению с СКЗИ

1. Общие положения

Настоящая Инструкция разработана в целях регламентации действий лиц, допущенных к работе со средствами криптографической защиты информации (СКЗИ) в организациях, которые осуществляют работы с применением СКЗИ (далее – Организация).

Под Организацией в настоящей Инструкции понимаются ГБОУ РК «Ливадийская санаторная школа-интернат».

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

Под обращением с СКЗИ в настоящей Инструкции понимается проведение мероприятий по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

СКЗИ должны использоваться для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

Функции органа криптографической защиты информации для проведения мероприятий по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации ограниченного доступа возложены на УФК по Республике Крым.

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) и «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.

2. Термины и определения

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами;

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, разрабатывающая и осуществляющая мероприятия по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации ограниченного доступа.

Персональный компьютер (ПК) - вычислительная машина, предназначенная для эксплуатации пользователем Организации в рамках исполнения должностных обязанностей.

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.

2. Работа с СКЗИ

Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях пользователей СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ. На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае, в организации должны быть обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется, после получения ключевых носителей, создать рабочие копии. Копии должны быть соответствующим образом маркированы и должны использоваться, учитываться и храниться так же, как оригиналы. Рекомендуется хранить копию криптоключей у администратора безопасности в опечатанном воде с фиксацией в соответствующем журнале. Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и оттисков печати.

Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ и (или) сотрудниками ОКЗ под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями СКЗИ должна быть санкционирована ОКЗ. Организация с согласия ОКЗ может разрешить передачу СКЗИ, документации к ним, ключевых документов между допущенными к СКЗИ лицами по актам без обязательной отметки в журнале поэкземплярного учета.

При обнаружении на рабочем месте, оборудованном СКЗИ, посторонних программ или вирусов, нарушающих работу указанных средств, работа со средствами защиты информации на данном рабочем месте должна быть прекращена и организуются мероприятия по анализу и ликвидации негативных последствий данного нарушения.

3. Порядок хранения и использования СКЗИ

1) Рекомендуется хранить ключевые носители в помещениях, которые имеют прочные входные двери с установленными на них надежными замками.

2) При использовании в качестве ключевых носителей криптоключей не защищённых устройств (flash, CD-карты и др.) в обязательном порядке для хранения ключевых носителей в помещении должно использоваться металлическое хранилище (сейф, шкаф, секция) заводского изготовления, оборудованное приспособлением для его опечатывания. Опечатывание хранилища должно производиться личной печатью ответственного

исполнителя криптоключей или его владельца.

3) При использовании в качестве ключевых носителей криптоключей защищённых устройств (Rutoken, Touch-Memory и др.) специализированного хранилища для данного носителя не требуется, при условии соблюдения технических требований эксплуатации такого устройства. Данное техническое устройство должно иметь соответствующий сертификат соответствия ФСТЭК.

4) Хранение ключевых носителей допускается в одном хранилище с другими документами и ключевыми носителями, при этом отдельно от них и в упаковке, исключающей возможность негласного доступа к ним. Для этого ключевые носители помещаются в специальный контейнер, опечатываемый личной металлической печатью ответственного исполнителя или владельца;

5) Помещения, в которых эксплуатируются СКЗИ должны опечатываться ответственным ратником во внерабочее время с соответствующей записью в журнале опечатывания мест эксплуатации СКЗИ;

6) Транспортирование ключевых носителей за пределы организации допускается только в случаях, связанных с производственной необходимостью. Транспортирование ключевых носителей должно осуществляться способом, исключающим их утрату, подмену или порчу.

7) На технических средствах, оснащенных средствами СКЗИ, должно использоваться только лицензионное программное обеспечение фирм-производителей.

8) Должны быть приняты меры по исключению несанкционированного доступа посторонних лиц в помещения, в которых установлены технические средства СКЗИ;

9) Запрещается оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки (**в соответствии с политикой информационной безопасности**);

10) Ключевая информация содержит сведения конфиденциального характера, хранится на учтенных в установленном порядке носителях и не подлежит передаче третьим лицам;

11) Закрытые ключи изготавливаются в 2-х экземплярах: эталонная и рабочая копии. В повседневной работе используется рабочая копия ключевого носителя. Эталонная копия записывается на ключевой носитель, опечатывается и передаётся на хранение ответственному за информационную безопасность с соответствующей записью в журнале приёма-передачи либо хранитсмя у владельца в недоступном посторонним месте. Срок действия ключей устанавливается удостоверяющим центром;

12) При физической порче рабочей копии ключевого носителя, пользователь немедленно уведомляет об этом администратора безопасности. Администратор безопасности в присутствии пользователя изготовляет очередную рабочую копию ключевого носителя с эталонной копии с отражением выполненных действий в соответствующих учетных формах;

13) Ключевой носитель извлекается из опечатанного контейнера только на время работы с ключами. Перед вскрытием контейнера необходимо проверить целостность печати и ее принадлежность. В нерабочее время опечатанный контейнер с ключевыми носителями должен находиться в хранилище;

14) При необходимости временно покинуть помещение, в котором проводятся работы с использованием СКЗИ, ключевой носитель должен быть вновь помещён в контейнер и опечатан.

15) Категорически не допускается:

- .осуществлять несанкционированное администратором безопасности копирование ключевых носителей;
- разглашать содержимое ключевых носителей и передачу самих носителей лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей и принтер;
- использовать ключевые носители в режимах, не предусмотренных правилами пользования ЭП, либо использовать ключевые носители на посторонних ПЭВМ;
- записывать на ключевые носители постороннюю информацию

4. Действия в случае компрометации ключей

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации ограниченного доступа, пользователи СКЗИ обязаны сообщать Ответственному за организацию работ по криптографической защите информации.

К компрометации ключей относятся следующие события:

1) утрата носителей ключа;
2) утрата иных носителей ключа с последующим обнаружением;
3) увольнение сотрудников, имевших доступ к ключевой информации;
4) возникновение подозрений на утечку информации или ее искажение;
5) нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;
6) утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;
7) утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;
8) доступ посторонних лиц к ключевой информации;
9) другие события утери доверия к ключевой документации.

Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия.

Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения). В случаях недостачи, не

предъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

Мероприятия по розыску и локализации последствий компрометации информации ограниченного доступа, передававшейся (хранящейся) с использованием СКЗИ, организует и осуществляет Организация (обладатель скомпрометированной информации ограниченного доступа).

5. Обязанности и ответственность лиц, допущенных к работе с СКЗИ

Лица, допущенные к работе с СКЗИ, обязаны:

1) Не разглашать информацию ограниченного доступа, к которой они допущены, в том числе сведения о криптоключах;
2) Сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;
3) Соблюдать требования к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;
4) Сообщать в ОКЗ о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
5) Немедленно уведомлять 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.
6) В случае необходимости производить уничтожение криптоключей и ключевых документов в соответствии с требованиями пунктов 41-46 Инструкции ФАПСИ от 13 июня 2001 г. №152 и уведомлять об этом ОКЗ.
7) Не вводить номера лицензий на СКЗИ, уже вводимые на других АРМ.

Лица, допущенные к работе с СКЗИ, отвечают за исполнение своих функциональных обязанностей и сохранность информации ограниченного доступа, которая стала ему известной вследствие исполнения им своих служебных обязанностей.

1. Ответственные исполнители ЭП при работе с ключевыми документами обязаны руководствоваться положениями соответствующего Регламента Удостоверяющего центра и настоящей Инструкции.
2. Ответственные исполнители ЭП обязаны организовать свою работу по генерации ЭП в полном соответствии с положениями соответствующего Регламента Удостоверяющего центра и данной инструкции.
3. Ответственные исполнители ЭП обязаны организовать свою работу с ключевыми документами в полном соответствии настоящей Инструкцией.
4. Уничтожение ключевой информации с ключевого носителя может производится только в полном соответствии с положениями соответствующего Регламента Удостоверяющего центра и настоящей Инструкцией.
5. Ответственные исполнители ЭП обязаны выполнять требования Администратора безопасности информации в части, касающейся обеспечения информационной безопасности Организации.

Ответственность лиц, допущенных к работе с СКЗИ, за неисполнение и (или)

ненадлежащее исполнение своих обязанностей, предусмотренных соответствующими инструкциями (Инструкция ответственного за организацию работ по криптографической защите информации, Инструкция пользователя СКЗИ), а также за разглашение информации ограниченного доступа, ставшей ему известной вследствие исполнения им своих служебных обязанностей, определяется действующим законодательством Российской Федерации и условиями трудового договора.

С инструкцией ознакомлены (ответственные за работу со СКЗИ):

№	ФИО	Подпись	Дата ознакомления