ДЕПАРТАМЕНТ СОЦИАЛЬНОЙ ПОЛИТИКИ И ЗАНЯТОСТИ НАСЕЛЕНИЯ БРЯНСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ БРЯНСКОЙ ОБЛАСТИ «КОМПЛЕКСНЫЙ ЦЕНТРСОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ НАСЕЛЕНИЯ ДУБРОВСКОГО РАЙОНА»

ПРИКАЗ

22.11.2023 г. № 98

Об организации работы со средствами криптографической защиты информации (СКЗИ) в ГБУ КЦСОН Дубровского района

В целях исполнения требований по организации и обеспечению функционирования СКЗИ, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённых следующими нормативными документами:

- приказом ФАПСИ 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»,

- приказом ФСБ России от 21.02.2008 № 149/6/6-622 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации»

ПРИКАЗЫВАЮ:

1. Назначить ответственным за эксплуатацию средств криптографической защиты информации (далее – Ответственный) гл. бухгалтера Сивачеву Наталью Алексеевну.

2. Определить что, при отсутствии Ответственного его обязанности по работе с СКЗИ исполняет бухгалтера Сидукина Наталья Александровна.

3. Утвердить «Инструкцию по работе ответственного за обеспечение безопасности использования средств криптографической защиты информации (СКЗИ) в ГБУ КЦСОН Дубровского района» (Приложение 1).

4. Ответственному за эксплуатацию СКЗИ руководствоваться данной Инструкцией при организации и обеспечении работы с СКЗИ и криптографическими ключами сотрудников, имеющих допуск к работе с СКЗИ в ГБУ КЦСОН Дубровского района.

4. Утвердить форму «Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов» (Приложение 2).

5. Утвердить форму «Лицевого счета пользователя средств криптографической защиты информации» (Приложение 3).

6. Ответственному за эксплуатацию СКЗИ обеспечить ознакомление сотрудников, допущенных к работе с СКЗИ с правилами работы с СКЗИ.

7. Возложить на сотрудника, ответственного за эксплуатацию СКЗИ, контроль за допуском лиц к работе с СКЗИ, предназначенных для обеспечения безопасности персональных данных в управлении, в соответствии с настоящим Приказом.

8. Контроль исполнения настоящего оставляю за собой.

Директор
ГБУ КЦСОН Дубровского района Н.В. Трифонова

Приложение 1
к приказу ГБУ КЦСОН Дубровского района
от 22.11.2023 № 98

Инструкция
по работе ответственного за обеспечение безопасности использования средств криптографической защиты информации (СКЗИ)
в ГБУ КЦСОН Дубровского района

Обозначения и сокращения

АРМ – автоматизированное рабочее место;
НСД – несанкционированный доступ;
ОС – операционная система;
ПДн – персональные данные;
СКЗИ – средства криптографической защиты информации.

Введение

Настоящая Инструкция определяет порядок учета, хранения и использования СКЗИ и криптографических ключей, а также порядок изготовления, смены, уничтожения и компрометации криптографических ключей в целях обеспечения безопасности персональных данных в ГБУ КЦСОН Дубровского района (далее – Учреждение).

Действие настоящей Инструкции распространяется на всех сотрудников Учреждения, допущенных к работе с СКЗИ.

1. Общие положения

1.1. Для организации и обеспечения работ по техническому обслуживанию СКЗИ и управления криптографическими ключами назначается Ответственный за эксплуатацию СКЗИ (далее – Ответственный).

1.2. Ответственный осуществляет:

- поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним;
- учёт сотрудников Учреждения допущенных к работе с СКЗИ (далее – Пользователи СКЗИ);
- контроль за соблюдением условий использования СКЗИ;
- расследование и составление заключения по фактам нарушения условий использования СКЗИ;
- разработку и принятие мер по предотвращению возможных последствий таких нарушений.

1.3. Пользователи СКЗИ назначаются в установленном порядке приказом руководителя Учреждения.

1.4. Пользователь СКЗИ обязан:

- не разглашать информацию, к которой допущен, в том числе сведения о криптографических ключах;
- соблюдать требования по обеспечению безопасности информации при использовании СКЗИ;

- сдать СКЗИ, эксплуатационную и техническую документацию к ним, криптографические ключи в соответствии с порядком, установленным настоящей Инструкцией, при прекращении использования СКЗИ;
- незамедлительно уведомлять Ответственного о фактах утраты или недостачи СКЗИ, криптографических ключей, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемой информации, а также о причинах и условиях ее возможной утечки.

1.5. Непосредственно к работе с СКЗИ Пользователи допускаются только после соответствующего обучения.

1.6. Обучение Пользователей правилам работы с СКЗИ осуществляет Ответственный или другой сотрудник, назначенный приказом руководителя Учреждения.

1.7. Текущий контроль, обеспечение безопасного функционирования СКЗИ возлагается на Ответственного.

1.8. Ответственный и Пользователи СКЗИ должны быть ознакомлены с настоящей Инструкцией под подпись.

2. Учет и хранение СКЗИ и криптографических ключей

2.1. СКЗИ, эксплуатационная и техническая документация к ним, криптографические ключи подлежат поэкземплярному учету.

2.2. Поэкземплярный учет ведет Ответственный в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (приложение 1). При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное использование.

2.3. Единицей поэкземплярного учета криптографических ключей считается отчуждаемый ключевой носитель.

2.4. Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, криптографические ключи должны быть выданы под подпись в журнале Пользователям СКЗИ. Пользователи СКЗИ несут персональную ответственность за сохранность полученных СКЗИ.

2.5. Криптографические ключи хранятся у Пользователей СКЗИ. Хранение осуществляется в сейфах (шкафах, ящиках) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

2.6. Ключевые носители с неработоспособными криптографическими ключами Ответственный принимает от Пользователя СКЗИ под подпись в описи криптографических ключей Пользователя СКЗИ) и в журнале поэкземплярного учета ключевых документов. Неработоспособные ключевые носители подлежат уничтожению.

2.7. Аппаратные средства, с которыми осуществляется штатное использование СКЗИ, а также аппаратные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы).

2.8. Закрытые криптографические ключи не передаются.

2.9. Ключевые носители совместно с описью криптографических ключей должны храниться Пользователем СКЗИ в сейфе (металлическом шкафу).

3. Использование СКЗИ и криптографических ключей

3.1. Для обеспечения контроля доступа к СКЗИ системный блок АРМ опечатывается Ответственным.

3.2. Пользователь СКЗИ должен ежедневно проверять сохранность оборудования и целостность печатей на АРМ.

3.3. В случае обнаружения не зарегистрированных программ или факта повреждения целостности печати на системном блоке АРМ, работа с СКЗИ на данной АРМ должна быть прекращена. По данному факту проводится служебное расследование, осуществляются работы по анализу и ликвидации последствий данного нарушения.

3.4. Правом доступа к АРМ с установленными СКЗИ должны обладать только определенные для эксплуатации лица, прошедшие соответствующую подготовку. Ответственный должен ознакомить каждого Пользователя СКЗИ, с документацией на СКЗИ, а также с другими нормативными документами, созданными на её основе.

3.5. Защита информации от НСД должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

3.6. К установке общесистемного и специального программного обеспечения, а также СКЗИ, допускаются лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее программное обеспечение и на СКЗИ.

3.7. При установке программного обеспечения СКЗИ следует:

- на технических средствах, предназначенных для работы с СКЗИ, использовать только лицензионное программное обеспечение;
- при установке СКЗИ на АРМ должен быть обеспечен контроль целостности и достоверность дистрибутива СКЗИ;
- не устанавливать на АРМ средства разработки программного обеспечения и отладчики;
- после завершения процесса установки выполнить действия, необходимые для осуществления периодического контроля целостности установленного СКЗИ, а также его окружения в соответствии с документацией.

3.8. Программное обеспечение, устанавливаемое на АРМ с СКЗИ не должно содержать возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;
- модифицировать собственный код и код других подпрограмм;
- модифицировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;
- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- повышать предоставленные привилегии;
- модифицировать настройки ОС;
- использовать недокументированные функции ОС.

3.9. При организации работ по защите информации от НСД необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п .);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях;
- личный пароль Пользователь не имеет права сообщать никому;
- периодичность смены пароля не должна превышать 90 дней.

3.10. Средствами BIOS должна быть исключена возможность работы на АРМ с СКЗИ, если во время её начальной загрузки не проходят встроенные тесты.

3.11. Уполномоченный сотрудник должен сконфигурировать операционную систему, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

- не использовать нестандартные, измененные или отладочные версии ОС;
- исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой;
- исключить возможность удаленного управления, администрирования и модификации ОС и её настроек;
- на АРМ должна быть установлена только одна ОС;
- правом установки и настройки СКЗИ должен обладать только Ответственный;
- все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т. п.);
- режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень;
- всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права.

3.12. Необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):

- системный реестр;
- файлы и каталоги;
- временные файлы;
- журналы системы;
- файлы подкачки;
- кэшируемая информация (пароли и т.п.);
- отладочная информация.

3.13. Необходимо организовать затирание (по окончании сеанса работы СКЗИ) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ. Если это не выполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.

3.14. Должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии.

3.15. Необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС.

3.16. В случае подключения АРМ с установленным СКЗИ к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (например, JavaScript, VBScript, ActiveX), полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

3.17. При использовании СКЗИ на АРМ, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых ОС к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например: установка
межсетевых экранов, организация VPN сетей и т.п.). При этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации.

3.18. Необходимо организовать и использовать систему аудита, проводить регулярный анализ результатов аудита.

3.19. ЗАПРЕЩАЕТСЯ:

- оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации;
- вносить какие-либо изменения в программное обеспечение СКЗИ;
- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации (за исключением случаев, предусмотренных данными правилами);
- использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;
- записывать на ключевые носители постороннюю информацию;
- вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом использования ключевого носителя;
- подключать к АРМ дополнительные устройства и соединители, не предусмотренные штатной комплектацией;
- вносить какие-либо изменения в программное обеспечение СКЗИ;
- изменять настройки, установленные программой установки СКЗИ;
- использовать синхропосылки, вырабатываемые не средствами СКЗИ;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ;
- осуществлять несанкционированное вскрытие системных блоков АРМ.

4. Действия при компрометации криптографических ключей

4.1. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

- потеря ключевых носителей;
- потеря ключевых носителей с их последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нарушение печати на сейфе с ключевыми носителями;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

4.2. В случае возникновения обстоятельств, указанных в п. 4.1 настоящей Инструкции, Пользователь СКЗИ обязан немедленно прекратить обмен электронными документами с использованием скомпрометированных закрытых криптографических ключей и сообщить о факте компрометации Ответственному.

4.3. Смена криптографических ключей проводится в соответствии с положениями регламентов удостоверяющих центров, которыми они были выданы.

4.4. Использование СКЗИ может быть возобновлено только после ввода в действие другого криптографического ключа взамен скомпрометированного.

4.5. Скомпрометированные ключи подлежат уничтожению в соответствии с порядком, установленным в разделе 5 настоящей Инструкции.

5. Уничтожение криптографических ключей

5.1. Неиспользованные или выведенные из действия криптографические ключи подлежат уничтожению.

5.2. Уничтожение криптографических ключей на ключевых носителях производится комиссией, назначенной руководителем Учреждения.

5.3. Криптографические ключи, находящиеся на ключевых носителях, уничтожаются путем их стирания в соответствии с требованиями эксплуатационной и технической документации на СКЗИ.

5.4. При уничтожении криптографических ключей, находящихся на ключевых носителях, комиссия обязана:

- установить наличие оригинала и количество копий криптографических ключей;
- проверить внешнюю целостность каждого ключевого носителя;
- идентифицировать каждый ключевой носитель в соответствии с журналом поэкземплярного учета;
- убедиться, что криптографические ключи, находящиеся на ключевых носителях, действительно подлежат уничтожению;
- произвести уничтожение криптографических ключей на оригинале и всех копиях ключевого носителя.

5.5. О факте уничтожения криптографических ключей составляется акт об уничтожении криптографических ключей.

5.6. Акт об уничтожении криптографических ключей подписывается членами комиссии и председателем комиссии.

5.7. В журнале поэкземплярного учета Ответственным производится отметка об уничтожении криптографических ключей с указанием даты уничтожения и номера акта.

5.8. Акты об уничтожении криптографических ключей СКЗИ хранятся у Ответственного.

6. Требования к помещениям, в которых ведется работа с СКЗИ или хранятся криптографические ключи

6.1. Помещения, в которых расположены АРМ, на которых ведется работа с СКЗИ или в которых хранятся криптографические ключи (далее - помещения), должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, необходимо оборудовать охранной сигнализацией, решетками или другими средствами, препятствующими неконтролируемому проникновению в помещения.

6.2. Охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

6.3. Двери помещений должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей.

6.4. Окна помещений должны быть защищены для предотвращения просмотра извне.

6.5. В помещении для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей должно быть предусмотрено необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у сотрудника, ответственного за хранилище. Дубликаты ключей от хранилищ должны храниться в сейфе Ответственного или в сейфе руководителя Учреждения.

6.6. По окончании рабочего дня помещения и установленные в них хранилища должны быть закрыты, хранилища опечатаны.

6.7. При утрате ключа от хранилища или от входной двери в помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить.

6.8. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, должно быть немедленно сообщено Ответственному за обеспечение безопасности персональных данных при их обработке в ИСПДн.

Приложение 2
к приказу ГБУ КЦСОН Дубровского района
от 22.11.2023 № 98

Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов

(ФОРМА)

№ п/п	Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводи-тельного документа	Ф.И.О. пользователя криптосредств	Дата и расписка в получении
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Наименование организации, Ф.И.О. сотрудника, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены криптосредства	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписки об уничтожении	
9	**10**	**11**	**12**	**13**	**14**	**15**

Приложение 3

к приказу ГБУ КЦСОН Дубровского района
от 22.11.2023 № 98

Лицевой счет пользователя
средств криптографической защиты информации
(ФОРМА)

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о передаче		Отметка о возврате, уничтожении		Примечание
				От кого получены	Дата и расписка в получении	Кому передано СКЗИ	Дата и расписка в передаче	Дата возврата (уничтожения)	Расписка о возврате (уничтожении)	
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**