УТВЕРЖДЕНО
приказом директора
МАУ ТЦ «ТенХауС»
от «12» сентября 2016 г.
№ 09-б

ИНСТРУКЦИЯ
по обращению с шифровальными (криптографическими) средствами защиты информации в муниципальном автономном учреждении «Теннисный центр «ТенХауС»

1. Общие положения

1.1. Настоящая инструкция регламентирует порядок обращения с шифровальными (криптографическими) средствами, предназначенными для защиты информации, не содержащей сведений, составляющих государственную тайну, в процессе их получения, транспортировки, учета, хранения, уничтожения, а также порядок допуска к работам с шифровальными средствами.

1.2. К шифровальным (криптографическим) средствам (средствам криптографической защиты информации – СКЗИ) относятся:

- средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации от несанкционированного доступа при ее передаче по каналам связи и (или) при ее обработке и хранении;
- средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;
- средства электронной подписи (ЭП) – аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием закрытого ключа электронной, подтверждение с использованием открытого ключа электронной подписи подлинности электронной подписи, создание закрытых и открытых ключей электронной подписи;
- средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций.

1.3.Сотрудники муниципального автономного учреждения «Теннисный центр «ТенХауС» (далее –Учреждение) допускаются к работе с СКЗИ на основании приказов директора Учреждения после прохождения необходимой подготовки.

1.4. В Учреждении должно быть назначено приказом лицо, ответственное за обеспечению безопасности эксплуатации средств криптографической защиты информации.

1.5. Ответственный назначается и освобождается от исполнения обязанностей, предусмотренных настоящей инструкцией и другими организационно-

распорядительными документами Учреждения, приказом директора Учреждения или лицом, исполняющим обязанности директора.

1.6. Ответственный в своей работе непосредственно подчиняется директору Учреждения.

1.7. Функциональными обязанностями Ответственного являются:

- взаимодействие с органами лицензирования и сертификации ФСБ России, разработчиками (производителями) СКЗИ и поставщиками услуг в области шифрования информации;
- разработка и практическое осуществление мероприятий по обеспечению функционирования и безопасности СКЗИ, в том числе открытых и закрытых ключей шифрования (криптоключей), электронной подписи (ЭП) и сертификатов открытых ключей;
- координация и контроль деятельности операторов СКЗИ при работе с СКЗИ;
- разработка и участие в согласовании технической и организационно-распорядительной документации, связанной с применением СКЗИ в Учреждении;
- ведение журнала поэкземплярного учета СКЗИ;
- участие в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации, в том числе в случае компрометации действующих криптоключей;
- участие в разборе конфликтных ситуаций;
- доклад непосредственному руководителю о выявленных нарушениях операторов СКЗИ и/или сотрудников Учреждения и/или третьих лиц в отношении СКЗИ, а также о принятие необходимых мер по устранению данных нарушений.

1.8. Все сотрудники Учреждения, допущенные к работе с СКЗИ, должны ознакомиться с настоящей инструкцией под роспись и строго выполнять требования следующих документов:

- настоящая инструкция;
- эксплуатационная документация на СКЗИ;
- организационно-распорядительные документы Учреждения, связанными с СКЗИ.

1.9. Разработка и проведение мероприятий по обеспечению безопасности при проведении работ с СКЗИ осуществляется лицом, уполномоченным руководить работами с СКЗИ (ответственным за обеспечению безопасности эксплуатации средств криптографической защиты информации).

2. Требования по размещению, специальному оборудованию и охране помещений, в которых производятся работы с СКЗИ

2.1. Размещение, специальное оборудование, охрана и режим в помещениях, в которых ведется работа с СКЗИ (далее – помещения), должны обеспечивать безопасность информации, СКЗИ, путем сведения к минимуму возможности неконтролируемого доступа к СКЗИ, просмотра процедур работы с СКЗИ посторонними лицами.

2.2. Порядок допуска в помещения определяется внутренней организационно-распорядительной документацией Учреждения. Доступ лиц в эти помещения должен быть ограничен в соответствии со служебной необходимостью. Рекомендуется использовать технические системы ограничения доступа в эти помещения. Допуск в помещения вспомогательного и обслуживающего персонала (уборщиц, электромонтеров, сантехников и т.д.) производится только в случае

служебной необходимости в сопровождении ответственного за режим после принятых мер, исключающих визуальный просмотр конфиденциальных документов.

2.3. Входные двери помещений должны быть прочными и оборудованы замками, гарантирующими надежное закрытие помещений в нерабочее время. Для контроля за входом в рабочее время рекомендуется устанавливать элементы систем контроля доступа.

2.4. При расположении помещений на первых и последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц и т.п., окна помещений оборудуются металлическими решетками, ставнями, охранной сигнализацией или другими средствами, препятствующими несанкционированному доступу в помещения.

2.5. Для предотвращения просмотра извне окна помещений должны быть защищены (оборудованы жалюзи или шторами и т.п.).

2.6. Внутренняя планировка и расположение рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений.

2.7. По окончании рабочего дня помещения закрываются и сдаются под охрану.

2.8. В случае утраты ключа от входной двери помещения директор Учреждения немедленно ставится в известность.

2.9. Для непосредственного хранения СКЗИ, носителей, эксплуатационной и технической документации к СКЗИ помещения обеспечиваются металлическими шкафами (хранилищами, сейфами), оборудованными внутренними замками с двумя экземплярами ключей или кодовыми замками, а также при необходимости приспособлениями для опечатывания замочных скважин.

3. Порядок обращения со средствами криптографической защиты информации

3.1. СКЗИ, получает уполномоченный сотрудник Учреждения непосредственно у производителя СКЗИ или организации, предоставляющей СКЗИ. Безопасность в процессе доставки обеспечивается организационными мерами.

3.2. При транспортировке СКЗИ, инсталлирующих СКЗИ носителей, должны быть обеспечены условия, исключающие возможность физических повреждений и внешнего воздействия на записанную информацию, а также ее копирование.

3.3. Все поступающие СКЗИ, инсталлирующие СКЗИ носители, эксплуатационная и техническая документация к ним должны браться на поэкземплярный учет в специальных журналах установленной формы. Ведет журналы уполномоченный на это сотрудник.

3.4. Инсталлирующие СКЗИ носители должны храниться в сейфе (металлическом шкафу, хранилище).

3.5. При вскрытии сейфа с инсталлирующими СКЗИ носителями должна быть проверена целостность печатей и замков и/или оттисков печатей. В случае нарушения целостности печатей и/или замков и/или оттисков печатей сотрудник обязан немедленно сообщить об этом лицу, ответственному за обеспечению безопасности эксплуатации средств криптографической защиты информации.

3.6. Хранение инсталлирующих СКЗИ носителей допускается в одном хранилище с другими документами при условиях, исключающих

непреднамеренное их уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение.

3.7. В случае отсутствия у сотрудника индивидуального хранилища инсталлирующие СКЗИ носители по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.

3.8. Не допускается:

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер; вставлять ключевой носитель в дисковод ПЭВМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровка информации, заверка файлов ЭП, подтверждение ее подлинности), а также в дисководы других ПЭВМ
- записывать на ключевом носителе постороннюю информацию;
- вносить какие-либо изменения в программное обеспечение средств шифрования и ЭП;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей).

3.9. Посторонние лица не должны допускаться к работе с компьютером, на котором установлены СКЗИ.

3.10. Пользователь СКЗИ несет ответственность за проведение в полном объеме организационных и технических мероприятий, обеспечивающих выполнение настоящей Инструкции

4. Установка и эксплуатация средств криптографической защиты информации

4.1. Установка (инсталляция) СКЗИ осуществляется в соответствии с требованиями документации на СКЗИ.

4.2. Установка СКЗИ производится только лицами, имеющими соответствующие полномочия и подготовку.

4.3. К эксплуатации СКЗИ и средств ЭП допускаются лица, прошедшие соответствующую подготовку и изучившие эксплуатационную документацию на данные СКЗИ.

4.4. Перед установкой СКЗИ необходимо проверить программное обеспечение ПЭВМ на отсутствие вирусов и программных закладок.

4.5. Системные блоки ПЭВМ с установленными СКЗИ должны опечатываться специально выделенной для этих целей печатью. Наряду с этим допускается применение других средств контроля их вскрытия.

4.6. Размещение и установка СКЗИ осуществляются в соответствии с требованиями документации на СКЗИ. Размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации должно соответствовать требованиям техники безопасности, санитарным нормам, а также требованиям пожарной безопасности.

4.7. Перед непосредственной установкой программного обеспечения СКЗИ необходимо осуществить контроль целостности дистрибутива. После завершения процесса установки должны быть выполнены действия, необходимые для осуществления ежедневного контроля установленного программного обеспечения, а также его окружения.

4.8. В случае обнаружения «посторонних» (не зарегистрированных) программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на ПЭВМ с СКЗИ должна быть прекращена. По данному факту должно быть проведено служебное расследование и проведены работы по анализу и ликвидации негативных последствий данного нарушения.

4.9. Пересылка (передача) носителей криптоключей может осуществляться через фельдъегерскую или специальную связь, а также со специально выделенным нарочным (в опечатанном Ответственным конверте).

4.10. Ключевая информация на носителях уничтожается оператором СКЗИ путем переформатирования с использованием средств ЭП. Допускается данные носители после переформатирования использовать в дальнейшем операторами СКЗИ при условии записи на них новой ключевой информации.

4.11. Об уничтожении ключей операторами СКЗИ делается соответствующая запись в соответствующем журнале. Периодически Ответственный проверяет данные записи.

4.12. Перед уничтожением секретных ключей следует расшифровать архивную информацию (если такая имеется), хранящуюся в зашифрованном виде, и зашифровать ее используя новые ключи.

5. Восстановление конфиденциальной связи после компрометации действующих криптоключей

5.1. Компрометация ключевой информации» - это утрата (в том числе с их последующим обнаружением), хищение, разглашение, несанкционированное копирование, передача их по линии связи в открытом виде, увольнение по любой причине сотрудника, имеющего доступ к ключевым носителям или к ключевой информации на данных носителях, любые другие виды разглашения ключевой информации, в результате которых закрытые ключи могут стать доступными несанкционированным лицам и (или) процессам.

5.2. К событиям, связанным с компрометацией криптоключей, относятся следующие:

- потеря ключевых носителей;
- потеря ключевых носителей с их последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил хранения и уничтожения секретного ключа;
- возникновение подозрений на утечку информации или ее искажение;
- нарушение печати на сейфе с ключевыми носителями (если такая используется);
- случаи, когда нельзя достоверно установить, что произошло с магнитными носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

5.3. Первые четыре события должны трактоваться как явная компрометация криптоключей. Три следующих события требуют специального рассмотрения в каждом конкретном случае.

5.4. При обнаружении признаков, указывающих на возможную компрометацию закрытых ключей, носителей и/или конфиденциальной информации, Оператор СКЗИ должен самостоятельно определить факт компрометации и оценить значение

этого события, после чего обязан немедленно оповестить лицо, Ответственное за обеспечение безопасности эксплуатации СКЗИ.

5.5. Ответственный обязан сообщить о компрометации Директору Учреждения.

5.6. Ответственный обязан оперативно оповестить всех операторов СКЗИ о факте (или предполагаемой) компрометации.

5.7. Расследование факта (или предполагаемой) компрометации должно проводиться на месте происшествия уполномоченными лицами.

5.8. Результатом рассмотрения является квалификация или не квалификация данного события как компрометация действующих криптоключей.

5.9. При установлении факта компрометации действующих криптоключей, скомпрометированные секретные ключи шифрования уничтожаются.

5.10. Ответственный должен оповестить остальных операторов СКЗИ о замене и сообщить им его открытые ключи.

6. Права и ответственность за нарушение требований Инструкции

6.1. Оператор СКЗИ имеет право:

- запрашивать и получать от сотрудников Учреждения сведения, справочные и другие материалы, необходимые для осуществления его деятельности.
- принимать участие в совещаниях по вопросам, входящим в его компетенцию (по решению Директора Учреждения);
- участвовать в семинарах (конференциях и т.п.) на темы «информационных технологий» и «защиты информации» в качестве слушателя;
- ставить перед руководством Учреждения вопросы о создании надлежащих условий для исполнения своих должностных обязанностей.

6.2. Ответственный имеет право:

- требовать от операторов СКЗИ безусловного соблюдения установленной технологии обработки электронных документов и выполнения инструкций по обращению с СКЗИ и обеспечению безопасности информации;
- инициировать обращение к руководству Учреждения с требованием о прекращении обработки информации в случаях нарушения установленной технологии обработки защищаемой информации или нарушения функционирования СКЗИ, средств и систем защиты информации;
- запрашивать и получать от операторов СКЗИ и/или сотрудников Учреждения сведения, справочные и другие материалы, необходимые для осуществления его деятельности;
- принимать участие в совещаниях по вопросам, входящим в его компетенцию (по решению директора Учреждения);
- участвовать в семинарах (конференциях и т.п.) на темы «информационных технологий» и «защиты информации» в качестве слушателя;
- вносить руководству Учреждения предложения по совершенствованию деятельности Учреждения в области шифрования информации;
- ставить перед руководством Учреждения вопросы о создании надлежащих условий для исполнения своих обязанностей.

6.3. Оператор СКЗИ несет ответственность (дисциплинарную, административную, материальную, уголовную) за:

- разглашение конфиденциальной информации, к которой он допущены, рубежи ее защиты, в том числе сведения о криптоключах;
- не соблюдение требований к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;

- не обеспечение сохранности принятых на ответственное хранение программных и технических СКЗИ;

- не соблюдение регламента эксплуатации СКЗИ;

- не сообщение руководству Учреждения о ставших ему известных попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним, а также 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 защищаемой конфиденциальной информации;

- ненадлежащее и несвоевременное выполнение своих функциональных обязанностей;

- не обеспечение сохранности принимаемой информации и достоверности передаваемой;

- несвоевременного, а также некачественного исполнения документов и поручений руководства Учреждения;

- нерациональное использование выделенных финансовых, материальных и информационно-вычислительных ресурсов.

6.4. Ответственный несет ответственность (дисциплинарную, административную, материальную, уголовную) за:

- не соблюдение требований к обеспечению безопасности информации ограниченного доступа с использованием СКЗИ;

- не обеспечение сохранности принятых на ответственное хранение программных и технических СКЗИ;

- не соблюдение регламента эксплуатации СКЗИ;

- не сообщение руководству Учреждения о ставших ему известных попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним, а также о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ;

- ненадлежащее и несвоевременное выполнение своих функциональных обязанностей;

- несвоевременного, а также некачественного исполнения документов и поручений руководства Учреждения;

- нерациональное использование выделенных финансовых, материальных и информационно-вычислительных ресурсов.