УТВЕРЖДЕНО:
Директор ОГАУ ДО ОСШ по футболу
(наименование общеобразовательной организации)

_____ /А.Ю. Фомин/
подпись расшифровка подписи

Приказ № 37 от 09.01.2024 г.

Инструкция
по обращению с криптографическими средствами защиты информации.

1. Общие положения.

1.1. Настоящая инструкция по обращению 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

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 подписи, 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 ОГАУ ДО ОСШ по футболу (далее-учреждение) допускаются к работе с СКЗИ после прохождения необходимой подготовки.

1.4. Лицо, ответственное за обеспечение безопасности эксплуатации средств криптографической защиты информации назначается и освобождается от исполнения обязанностей, предусмотренных настоящей инструкцией приказом руководителя учреждения.

1.5. Ответственное лицо в своей работе непосредственно подчиняется руководителю учреждения.

1.6. Функциональными обязанностями ответственного лица 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 учета экземпляров средств криптографической защиты информации и средств защиты информации учреждения (приложение 1); 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.

1.7. Все сотрудники, допущенные к работе со СКЗИ, должны ознакомиться с инструкцией по обращению под роспись и строго выполнять требования следующих документов: инструкции по обращению с криптографическими средствами защиты информации; эксплуатационной документации на СКЗИ; организационно-распорядительных документов учреждения, регламентирующих работу со СКЗИ.

1.8. Разработка и проведение мероприятий по обеспечению безопасности при проведении работ со СКЗИ осуществляется лицом, уполномоченным руководить данными работами (ответственным за обеспечение безопасности эксплуатации СКЗИ).

1.9. Пользователям, которым необходимо получить доступ к работе со СКЗИ, необходимо пройти самостоятельное обучение правилам указанной работы.

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 со СКЗИ (далее – помещения), должны обеспечивать безопасность информации СКЗИ путем сведения к минимуму возможности неконтролируемого к ним доступа и, просмотра процедур работы со 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 изготовлены из прочных материалов и оборудованы запирающими устройствами, 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 опечатываются и/или сдаются под охрану.

2.8. Сдачу ключей и помещений, а также получение ключей и вскрытие помещений производят сотрудники, работающие в этих помещениях, по утвержденному руководителем учреждения списку с образцами подписей этих

сотрудников. Дубликаты ключей от входных дверей должны храниться в сейфе ответственного лица, назначаемого руководителем учреждения.

2.9. Перед вскрытием помещений должна быть проверена целостность оттисков печатей и/или исправность замков. При обнаружении нарушения целостности оттисков печатей, повреждения замков или других признаков, указывающих на возможное проникновение в эти помещения посторонних лиц, помещение не вскрывается, а о случившемся немедленно ставится в известность руководство и отдел безопасности.

2.10. В случае утраты ключа от входной двери помещения руководитель учреждения немедленно ставится в известность.

2.11. На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, в которых предусматривается порядок вызова должностных лиц учреждения, вскрытия помещений, очередность и порядок спасения конфиденциальных документов и дальнейшего их хранения.

2.12. Для непосредственного хранения СКЗИ, носителей с дистрибутивами СКЗИ, 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. Уполномоченный сотрудник учреждения получает СКЗИ непосредственно у их производителя или организации, предоставляющей СКЗИ. Безопасность в процессе доставки обеспечивается организационными мерами.

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

3.3. Все поступающие СКЗИ, носители с дистрибутивами СКЗИ, эксплуатационная и техническая документация к ним должны браться на учет в специальных журналах установленной формы, ведение которых относится к компетенции уполномоченного сотрудника.

3.4. Носители с дистрибутивами СКЗИ должны храниться в сейфе (металлическом шкафу, хранилище).

3.5. При вскрытии сейфа, в котором хранятся носители с дистрибутивами СКЗИ, должна быть проверена целостность печатей и/или 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 обеспечение безопасности эксплуатации СКЗИ.

3.6. Хранение носителей с дистрибутивами СКЗИ 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 носители с дистрибутивами СКЗИ 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, не имеющим к ним допуска, выводить ключевую информацию на дисплей и принтер; вставлять ключевой носитель в дисковод ИСПДн при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровка информации, заверение файлов ЭП, подтверждение ее подлинности), а также в дисководы других ИСПДн; 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 по обращению.

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 (приложение 2 к инструкции по обращению с криптографическими средствами защиты информации).

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 ИСПДн на отсутствие вирусов и программных закладок.

4.5. Системные блоки ИСПДн 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 ИСПДн 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 в специально выделенном нарочному и опечатанном ответственным лицом конверте.

4.10. Ключевая информация на носителях уничтожается оператором СКЗИ путем переформатирования с использованием средств ЭП. После переформатирования допускается использование данных носителей операторами СКЗИ при условии записи на них новой ключевой информации.

4.11. Операторы СКЗИ делают запись об уничтожении ключей в учреждении в соответствующем журнале учета экземпляров средств криптографической защиты информации и средств защиты информации (приложение). Ответственное лицо периодически проверяет данные записи.

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

4.13. Выведенные из эксплуатации открытые ключи ЭП сохраняются в архивах в течение 5 (пяти) лет для обеспечения в последующем возможности выполнения процедуры разбора конфликтных ситуаций.

5. Восстановление конфиденциальной связи после компрометации действующих криптоключей.

5.1. Компрометация ключевой информации – это утрата или хищение действующих криптоключей (в том числе с их последующим обнаружением), разглашение или несанкционированное копирование ключевой информации, передача действующих криптоключей по линии связи в открытом виде, угроза разглашения ключевой информации вследствие увольнения по любой причине сотрудника, имеющего к ней доступ, а также 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: 1. утрата ключевых носителей; 2. хищение ключевых носителей; 3. обнаружение ключевых носителей после утраты или хищения; 4. увольнение сотрудников, имевших доступ к ключевой информации; 5. нарушение правил хранения и уничтожения секретного ключа; 6. возникновение подозрений на утечку информации или ее искажение; 7. нарушение печати на сейфе с ключевыми носителями; 8. случаи, когда нельзя достоверно установить, что произошло с магнитными носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и при этом не исключаются несанкционированные действия 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 немедленно оповестить.

5.5. Лицо, ответственное за обеспечение безопасности эксплуатации СКЗИ, обязано сообщить о компрометации закрытых ключей, носителей и/или конфиденциальной информации руководителю учреждения.

5.6. Лицо, ответственное за обеспечение безопасности эксплуатации СКЗИ, обязано 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 расследования является квалификация или отказ в квалификации данного события как компрометации действующих криптоключей.

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

5.10. Ответственное лицо должно оповестить остальных операторов СКЗИ о замене скомпрометированных криптоключей.

6. Права и ответственность за нарушение требований инструкции по обращению с криптографическими средствами защиты информации.

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 руководителя 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.Ответственное лицо имеет право:

требовать от операторов СКЗИ безусловного соблюдения установленной технологии обработки электронных документов и выполнения инструкций по обращению 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 администрации учреждения сведения, справочные и другие материалы, необходимые для осуществления его деятельности; принимать участие в совещаниях по вопросам, входящим в его компетенцию (по решению руководителя учреждения); участвовать в семинарах (конференциях и т.п.) об информационных технологиях и защите 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 допущен, рубежи ее защиты, в том числе сведения о криптоключах; несоблюдение требований по обеспечению безопасности конфиденциальной информации с использованием СКЗИ; необеспечение сохранности принятых на ответственное хранение программных и технических СКЗИ; несоблюдение регламента эксплуатации СКЗИ;

неинформирование руководства учреждения о ставших ему известных попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документов 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; необеспечение сохранности принимаемой и достоверности передаваемой информации; несвоевременное, а также некачественное исполнение документов и поручений руководства учреждения; нерациональное использование выделенных финансовых, материальных и информационно-вычислительных ресурсов.

6.4. Ответственное лицо несет уголовную, административную, дисциплинарную, гражданско-правовую и материальную ответственность, предусмотренную законодательством Российской Федерации, за: несоблюдение требований к обеспечению безопасности информации ограниченного доступа с использованием СКЗИ; необеспечение

сохранности принятых на ответственное хранение программных и технических СКЗИ;

несоблюдение регламента эксплуатации СКЗИ; неинформирование руководства учреждения о ставших ему известных попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документов 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; несвоевременное, а также некачественное исполнение документов и поручений руководства учреждения; нерациональное использование выделенных финансовых, материальных и информационно – вычислительных ресурсов.

Приложение 1
к Инструкции по обращению с
криптографическими средствами
защиты информации

Ж У Р Н А Л
учета экземпляров средств криптографической защиты информации и средств защиты информации
ОГАУ ДО ОСШ по футболу.

Журнал начат «____» _____ 20__ г.
Журнал завершен «____» _____ 20__ г.

Подпись, расшифровка_____/ _____/

Наименования граф:

1) №
2) Регистрационный номер
3) Наименование
4) Сведения об установке средства защиты информации
5) Сведения об изъятии/удалении средства защиты информации
6) Примечание
7) Дата установки
8) Место установки (использования)
9) Ф.И.О. производившего установку, подпись
10) Дата изъятия / удаления
11) Ф.И.О. производившего изъятие / удаление, подпись
12) Причина изъятия / удаления

Журнал учета СКЗИ
ОГАУ ДО ОСШ по футболу.

Журнал начат «____» _____ 20__ г.
Журнал завершен «____» _____ 20__ г.

Подпись, расшифровка_____/ _____/

Наименования граф:

1) №
2) Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов
3) Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов
4) Номера экземпляров (криптографические номера) ключевых документов
5) Отметка о получении
6) Отметка о выдаче
7) Отметка о подключении (установке СКЗИ)

8) Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов
9) От кого получены
10) Дата и номер сопроводительного письма
11) Ф.И.О. пользователя СКЗИ
12) Дата и расписка в получении (установка)
13) Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)
14) Дата подключения (установки) и подписи лиц, произведших подключение (установку)
15) Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ
16) Дата изъятия (уничтожения)
17) Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)
18) Номер акта или расписка об уничтожении

Приложение 2
к Инструкции по обращению с
криптографическими средствами
защиты информации

Форма о подготовке и допуске к самостоятельной работе со средствами криптографической защиты информации

_____ (Должность, фамилия, имя, отчество сотрудника)

_____
(Наименование СКЗИ, по которому осуществлялась подготовка)

Подготовка начата _____, окончена _____.

Оператор СКЗИ обязан: не разглашать конфиденциальную информацию, к которой допущен, рубежи ее защиты, в том числе сведения о криптоключах; соблюдать требования по обеспечению безопасности конфиденциальной информации с использованием СКЗИ; сообщать сотруднику, ответственному за эксплуатацию СКЗИ, сведения о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним; сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с установленным порядком при увольнении или отстранении от исполнения обязанностей сотрудников, связанных с использованием СКЗИ; немедленно уведомлять ответственного за обеспечение безопасности эксплуатации средств криптографической защиты информации о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ (сейфов), 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. Заключение – указать степень усвоения пройденного материала, результаты выполнения контрольных работ, возможность допуска к самостоятельной работы со СКЗИ.

С заключением ознакомлен(а):

_____ / _____

(Подпись) (ФИО)