



27.08.14

**РЕСПУБЛИКА КРЫМ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖИ
(МИНОБРАЗОВАНИЯ КРЫМА)**

П Р И К А З

от 22.08.2014

г. Симферополь

№ 2044

**Об организации работы с
системой криптографической
защиты информации,
используемой для обеспечения
безопасности персональных
данных, обрабатываемых в
Министерстве образования, науки
и молодёжи Республики Крым**

В соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», Приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Состав 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»

ПРИКАЗЫВАЮ:

1. Утвердить:

- 1) Инструкцию ответственного за обеспечение функционирования системы комплексной защиты информации (СКЗИ) (приложение 1);
- 2) Перечень пользователей СКЗИ (приложение 2);
- 3) Инструкцию пользователей СКЗИ (приложение 3);
- 4) Порядок организации контроля за соблюдением использования СКЗИ (приложение 4);
- 5) Журнал поэкземплярного учета СКЗИ (приложение 5)
- 6) Журнал учета доведения руководящих документов по организации и обеспечению функционирования шифровальных (криптографических) средств (приложение 6);

2. Назначить ответственным за обеспечение функционирования СКЗИ в Министерстве образования, науки и молодёжи Республики Крым ведущего специалиста отдела обеспечения информационно-технического сопровождения управления информационно-технического сопровождения ГКУ РК «Учреждение централизованного обслуживания» Бондаря Александра Васильевича (по согласованию).

3. Контроль за исполнением настоящего приказа оставляю за собой.

Министр



Н.Г. Гончарова

ИНСТРУКЦИЯ **ответственного за обеспечение функционирования системы комплексной защиты** **информации**

Раздел 1. Общие положения

1. Ответственный за обеспечение функционирования и безопасность применения средств криптографической защиты информации должен руководствоваться:

Федеральным законом "Об электронной подписи" от 06.04.2011 № 63-ФЗ;

Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (№ 149/54-144, 2008 года ФСБ России);

Инструкцией «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» (Приложение к Приказу Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 года № 152);

Приказом ФСБ России от 10.07.2014 № 378 "Об утверждении Составы 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"

эксплуатационно-технической документацией к средствам криптографической защиты информации;

настоящими функциональными обязанностями.

2. Ответственный за обеспечение функционирования и безопасность применения средств криптографической защиты информации подчиняется руководителю Учреждения.

На время отсутствия ответственного за обеспечение функционирования и безопасность применения средств криптографической защиты информации (отпуск, командировка, болезнь, пр.) его обязанности и права переходят к лицу, назначенному приказом руководителя организации.

Раздел 2. Обязанности

3. Ответственный за обеспечение функционирования и безопасность применения средств криптографической защиты информации обязан:

осуществлять руководство работой пользователей средств криптографической защиты информации;

– обеспечивать контроль за соблюдением пользователями средств криптографической защиты информации конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых средств криптографической защиты информации и ключевых документов к ним;

– контролировать выполнение пользователями правил эксплуатации средств криптографической защиты информации и соблюдением мер защиты от

несанкционированного доступа;

- осуществлять настройки средств криптографической защиты информации;
- назначать полномочия пользователей средств криптографической защиты информации;
- осуществлять контроль за попытками несанкционированного изменения режима безопасности, попытками несанкционированного доступа к программному обеспечению и попытками сетевых атак средств криптографической защиты информации;
- обеспечивать безопасное и надежное хранение средств криптографической защиты информации, эксплуатационной и технической документации к средствам криптографической защиты информации, ключевых документов;
- организовывать и проводить обучение пользователей средств криптографической защиты информации правилам работы с средствами криптографической защиты информации;
- немедленно принимать меры по предупреждению утечки защищаемых персональных данных, при выявлении фактов утраты или недостачи средств криптографической защиты информации, ключевых документов к ним, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.;
- осуществлять проверку целостности программного обеспечения и контроль за проведением регламентного тестирования средств криптографической защиты информации и обеспечения безопасности их использования;
- обеспечивать плановую смену ключей и смену ключей при компрометации;
- в случае компрометации ключевой информации немедленно прекратить конфиденциальную связь с другими абонентами (приостановить работу скомпрометированных средств криптографической защиты информации) и сообщить о факте компрометации (или предполагаемом факте компрометации) администратору безопасности Учреждения-организатора конфиденциальной связи;
- принимать своевременно меры по обеспечению безопасности информации и восстановлению конфиденциальной связи в случае компрометации (подозрении в компрометации) конфиденциальных ключей. Для восстановления конфиденциальной связи после компрометации ключей обращаться к администратору безопасности Учреждения-организатора конфиденциальной связи с целью регистрации вновь изготовленных (или резервных) ключей. Регистрация и выдача пользователям новых носителей ключевой информации и ЭЦП осуществляется тем же порядком, как и при плановой смене ключей.
- обеспечивать сохранность и конфиденциальность всей информации, которая станет ему известна при выполнении своих функций по пользованию информационной системой.

Раздел 3. Права

4. Ответственный за обеспечение функционирования и безопасность применения средств криптографической защиты информации имеет право:

- производить контроль обеспечения безопасности обращения со средствами криптографической защиты информации;
- вносить предложения руководителю Учреждения по улучшению работы средствами криптографической защиты информации;
- получать информацию, необходимую для выполнения своих обязанностей;
- участвовать в совещаниях, на которых рассматриваются вопросы обеспечения безопасности информации при эксплуатации средств криптографической защиты информации;
- принимать решения в пределах своей компетенции.

Раздел 4. Ответственность

5. При нарушениях руководителями и сотрудниками Министерства образования, науки и молодежи Республики Крым правил, связанных с безопасностью персональных данных, они несут ответственность, предусмотренную действующим законодательством Российской Федерации (ст. 24 Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»).

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

Ответственный за обеспечение функционирования и безопасность применения средств криптографической защиты информации отвечает за:

- соблюдение действующего законодательства, нормативных и руководящих документов в обеспечении функционирования и безопасности применения средств криптографической защиты информации;

- реализацию возложенных на него задач и функций;

- соблюдение правил учета и хранения средств криптографической защиты информации, ключевых документов, эксплуатационно-технической документации принятых на ответственное хранение и выданных для использования;

- сохранность средств криптографической защиты информации, ключевых документов, эксплуатационно-технической документации и документов, принятых на ответственное хранение и выдаваемых для использования;

- разглашение защищаемой законом конфиденциальной информации и персональных данных.

- соблюдение правил и норм охраны труда, пожарной безопасности, внутреннего трудового распорядка;

- обеспечение режима доступа в помещения, в которых установлены и (или) хранятся средства криптографической защиты информации и их охраны.

6. Ответственный за обеспечение функционирования и безопасность применения средств криптографической защиты информации несет ответственность за все действия, совершенные от имени своей учетной записи или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

**ПЕРЕЧЕНЬ ПОЛЬЗОВАТЕЛЕЙ
системы комплексной защиты информации**

1. Настоящий Перечень пользователей, допущенных к работе со средствами криптографической защиты информации, используемых для обеспечения безопасности персональных данных, обрабатываемых в информационной системе персональных данных «Регистрация документов об образовании, проведения ГИА и поступления в образовательные учреждения» Министерства образования, науки и молодежи Республики Крым разработан в соответствии с «Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, 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», утвержденными руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/6/6-622.

2. Перечень предназначен для организации допуска служащих Министерства образования, науки и молодежи Республики Крым к работе со средствами криптографической защиты информации.

3. Перечень может пересматриваться по мере необходимости в соответствии с установленным порядком.

№ п/п	Занимаемая должность	Ф.И.О. пользователя	Наименование и номер СКЗИ
1	Заместитель начальника управления— заведующий отделом среднего профессионального образования управления науки, среднего профессионального и высшего образования	А.Г. Артамонова	
2	Главный специалист отдела опеки и попечительства управления по защите прав несовершеннолетних	Г.А. Арифова	
3	Специалист-эксперт отдела лицензирования и государственной аккредитации образовательных учреждений управления по надзору и контролю за соблюдением законодательства в сфере образования	К.А. Дубовицкая	

ИНСТРУКЦИЯ **пользователей средств криптографической защиты информации**

Раздел 1. Общие положения

1. Настоящие Функциональные обязанности пользователя средств криптографической защиты информации (далее СКЗИ) разработаны в соответствии с:

Федеральным законом "Об электронной подписи" от 06.04.2011 № 63-ФЗ;

Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (№ 149/54-144, 2008 года ФСБ России);

Инструкцией «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» (Приложение к Приказу Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 года № 152);

Приказом ФСБ России от 10.07.2014 № 378 "Об утверждении Составы 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"

эксплуатационно-технической документацией к средствам криптографической защиты информации;

другими нормативными правовыми актами ФСБ России по вопросам обеспечения безопасности информации с использованием сертифицированных СКЗИ.

2. Под термином «пользователь» понимается служащий Министерства образования, науки и молодежи Республики Крым, допущенный в установленном порядке к работе с СКЗИ, используемых для обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных (ИСПДн).

3. Пользователи допускаются к работе с СКЗИ в соответствии с Перечнем, утвержденным настоящим приказом, после изучения и практического усвоения ими правил пользования и других руководств по эксплуатации СКЗИ.

Раздел 2. Обязанности

4. Пользователь СКЗИ обязан:

- строго соблюдать правила пользования программными, программно-аппаратными средствами криптографической защиты информации;
- осуществлять, в рамках предоставленных полномочий, регламентные проверки эксплуатации средств криптографической защиты информации;
- проводить проверку целостности программного обеспечения СКЗИ, системного, сетевого и прикладного программного обеспечения, в среде которого работают СКЗИ;
- не допускать установки на средства вычислительной техники (далее по тексту - СВТ), предназначенных для осуществления криптографической защиты информации, программного обеспечения, не относящегося к выполнению функциональных

обязанностей;

- использовать сертифицированные средства антивирусной защиты информации в целях предупреждения возможности заражения компьютерными вирусами и другими вредоносными программами;

- обеспечивать сохранность в тайне, от посторонних лиц информации о закрепленных за ним конфиденциальных ключевых документов;

- принимать своевременно меры по обеспечению безопасности информации и восстановлению конфиденциальной связи в случае компрометации (подозрении в компрометации) конфиденциальных ключей;

- обеспечивать сохранность и конфиденциальность всей информации, которая станет ему известна при выполнении своих функций по пользованию информационной системой.

- проводить проверку целостности программного обеспечения СКЗИ, системного, сетевого и прикладного программного обеспечения, в среде которого работают СКЗИ, должна выполняться пользователем после загрузки операционной системы при помощи программного обеспечения контроля целостности, входящего в состав программного обеспечения СКЗИ.

5. При эксплуатации СКЗИ запрещается:

- а) подключать к СВТ дополнительные устройства и оборудование без соответствующего предписания на возможность их совместного использования;

- б) работать на компьютере, если во время его начальной загрузки не проходит встроенный тест, предусмотренный в СВТ;

- в) оставлять без контроля вычислительные средства, входящие в состав СКЗИ, при включенном питании и загруженном программном обеспечении СКЗИ. При кратковременном перерыве в работе обязательно производить гашение экрана, возобновление активности экрана производится с использованием пароля доступа;

- г) вносить какие-либо изменения в программное обеспечение;

- д) несанкционированно устанавливать создавать и выполнять на СВТ посторонние программы;

- е) осуществлять несанкционированное вскрытие системных блоков СВТ.

Носители ключевой информации являются основным элементом, обеспечивающим стойкость конфиденциальной связи, поэтому при обращении с ключами Пользователь должен принять все необходимые меры, направленные на исключение несанкционированного доступа к ним.

6. При обращении с ключевой информацией пользователь СКЗИ обязан:

- хранить носители ключевой информации в сейфе (металлическом шкафу), имеющем приспособление для опечатывания;

- не оставлять носители ключевой информации без присмотра в устройствах (портах) ввода информации СВТ или на столе;

- получать/сдавать рабочие носители ключевой информации под роспись с указанием в журнале времени получения и сдачи;

- обращаться с письменным заявлением к ответственному за эксплуатацию СКЗИ для восстановления носителей ключевой информации с резервных копий, с указанием причин, повлекших необходимость восстановления.

7. Хранение конфиденциальных документов, носителей ключевой информации, нормативной и эксплуатационной документации разрешается только в металлических шкафах (хранилищах, сейфах). При вынужденных перерывах в работе носители ключевой информации и другие конфиденциальные документы должны быть закрыты в сейф, а сейф опечатан личной печатью.

8. Допускается хранение носителей ключевой информации в одном сейфе с другими документами в условиях, исключающих их непреднамеренное уничтожение или иное применение, не предусмотренное правилами пользования СКЗИ (на отдельной полке, в опечатанной папке или коробке).

9. Для защиты ключевой информации от механических, электромагнитных и

других факторов воздействия, приводящих к разрушению информации, либо ее искажению, целесообразно хранить дискеты в футлярах из экранирующего материала.

10. В случае отсутствия у Пользователя индивидуального хранилища, носители ключевой информации по окончании рабочего дня должны сдаваться на хранение ответственному за эксплуатацию СКЗИ под роспись.

11. При работе с ключевой информацией и ее носителями запрещается:

- а) снимать несанкционированные копии с носителей ключевой информации;
- б) разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным;
- в) выводить секретные ключи на дисплей, принтер или другие внешние устройства отображения информации;
- г) подключать носители ключевой информации (дискеты, USB флеш-накопители) к устройствам считывания (дисководы, USB-порты) в режимах, не предусмотренных штатным режимом, а также в устройства считывания (USB-порты) других СВТ, для этого не предназначенных;
- д) записывать на носители ключевой информации постороннюю информацию.

12. После плановой смены ключей или компрометации ключей пользователи СКЗИ уничтожают выведенные из действия носители ключевой информации со всех магнитных носителей не позднее чем через одни сутки после момента вывода ключей из действия.

13. При уничтожении ключей делается соответствующая запись в Журнале учета ключевых документов и ставятся росписи лиц, производивших уничтожение (стирание).

Раздел 3. Ответственность

При нарушениях служащими правил, связанных с безопасностью ПДн, они несут ответственность, предусмотренную действующим законодательством Российской Федерации (ст. 24 Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»).

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

Работники учреждения, имеющие доступ к персональным данным субъектов, виновные в незаконном разглашении или использовании персональных данных лиц без согласия субъектов из корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут уголовную ответственность в соответствии со ст. 183 Уголовного кодекса РФ.

Работники учреждения, имеющие доступ к персональным данным субъектов и совершившие указанный дисциплинарный проступок, несут полную материальную ответственность в случае причинения его действиями ущерба учреждению (п.7 ст. 243 Трудового кодекса РФ).

Порядок организации контроля за соблюдением использования СКЗИ

1. Настоящий порядок определяет структуру и содержание контрольных мероприятий за использованием шифровальных средств, применяемых для обеспечения безопасности персональных данных в соответствии с требованиями Приказа ФАПСИ от 13 июня 2001 г. № 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».

2. Для проверяющих лиц (штатные сотрудники или контролирующие органы) должен быть установлен объем допуска в ходе контрольных мероприятий.

3. При проведении контрольных мероприятий должностные лица вправе допускаться к таким объектам проверки, как:

- СКЗИ и средства защиты от несанкционированного доступа в автоматизированной системе;
- технические средства, на которых они реализованы;
- помещения, в которых установлены СКЗИ;
- технические средства защиты помещений;
- ключевые документы.

4. Структура контрольных мероприятий:

- организация системы организационных мер защиты персональных данных;
- организация системы криптографических мер защиты информации;
- проверка разрешительной и эксплуатационной документации;
- проверка выполнения требования к обслуживающему персоналу;
- проверка условий эксплуатации СКЗИ;
- оценка соответствия применяемых СКЗИ.

5. Организация системы организационных мер защиты ПДн включает:

- определение области применения средств криптографической защиты информации в ИСПДн;
- наличие ведомственных документов и приказов по организации криптографической ЗИ;
- выполнение рекомендаций и указаний ФСБ.

6. Организация системы криптографических мер защиты информации включает:

- наличие модели и угроз нарушителя;
- соответствие модели угроз исходным данным;
- соответствие требуемого уровня криптографической защиты полученной модели нарушителя;
- соответствие используемых СКЗИ полученному уровню криптографической защиты;

- наличие документов по поставке и внедрении СКЗИ оператору.

7. Проверка разрешительной и эксплуатационной документации включает:

- наличие лицензий;
- наличие сертификатов;
- наличие эксплуатационной документации на СКЗИ.

8. Порядок учета СКЗИ, эксплуатационной и технической документации включает: выявление несертифицированных ФСБ России средств.

9. Проверку выполнения требований к обслуживающему персоналу включает:

- проверку учета лиц;
- проверку наличия функциональных обязанностей пользователей СКЗИ, укомплектованность штатных должностей личным составом;
- проверка организации процесса обучения лиц, использующих СКЗИ, по вопросам организации работ с использованием СКЗИ.

10. Проверка условий эксплуатации СКЗИ включает:

- проверка правильности ввода СКЗИ в эксплуатацию;
- проверка соответствия условий эксплуатации (согласно эксплуатационной документации);
- проверка выполнения требований по размещению, оборудованию и охране, организации режима;
- проверка выполнения требований по соответствию режима доставки и хранения СКЗИ и ключевой документации предъявляемым требованиям;
- проверка наличия инструкций по восстановлению связи в случае компрометации действующих ключей к СКЗИ;

11. Оценка соответствия применяемых СКЗИ включает:

- контроль целостности файлов СКЗИ по эталонным контрольным суммам;
- проверка разграничения доступа к СКЗИ;
- проверка обеспечения конфиденциальности информации от утечки по каналам связи с использованием тестирующих программ;
- проверка прочих требований ФСБ по обеспечению безопасности с использованием СКЗИ.

12. Порядок проведения разбирательств и составления заключений по фактам нарушения условий хранения носителей ПДн или использования СКЗИ.

В акте проверки указываются следующие реквизиты:

- 1-дата и время и место составления акта;
- 2-Дата и номер распоряжения или приказа;
- 3-Фамилия имя отчество и должности, проводивших проверку;
- 4-Объект проверки;

5-Сведения о результатах проверки, в том числе и о выявленных нарушениях с лиц, на которые возлагается ответственность за это нарушение;

6-Сведения об ознакомлении или об отказе в ознакомлении с актом оператора, осуществляющего обработку персональных данных, а также лиц, присутствовавших при проведении проверки;

7-Дата время место проверки;

8-Подписи должностного лица или должностных лиц проводивших проверку.

К акту могут прилагаться протоколы, объяснения должностных лиц, на которых ответственность и другие документы о результатах проверки.

Приложение 6
к приказу Министерства образования,
науки и молодежи Республики Крым
от №

Журнал учета доведения руководящих документов по организации и обеспечению функционирования шифровальных (криптографических) средств

[illegible]