Областное государственное бюджетное учреждение
дополнительного профессионального образования
«Рязанский институт развития образования»
(ОГБУ ДПО «РИРО»)

РАССМОТРЕНО
на заседании ученого совета
ОГБУ ДПО РИРО
Протокол
от «20» 10 2015 г. № 6

УТВЕРЖДАЮ
Ректор ОГБУ ДПО «РИРО»
_____И.В.Костикова
«20» 10 2015 г.

СОГЛАСОВАНО с профкомом
(протокол от «19» 10 2015 г. № 7/15)
Председатель ППО ОГБУ ДПО «РИРО»
_____С.М.Горчакова

И Н С Т Р У К Ц И Я

по обращению с сертифицированными криптосредствами
в Областном государственном бюджетном учреждении
дополнительного профессионального образования
«Рязанский институт развития образования»
(ОГБУ ДПО «РИРО»)

г. Рязань, 2015 г.

Приложение № 1
к приказу от «__» _____ 20__ г. №_____

ИНСТРУКЦИЯ
по обращению с сертифицированными криптосредствами
в Областном государственном бюджетном учреждении дополнительного профессионального образования «Рязанский институт развития образования»
(ОГБУ ДПО «РИРО»)

1 Общие положения

1.1 Инструкция по обращению с сертифицированными криптосредствами, предназначенными для защиты информации, в том числе персональных данных, обрабатываемых в информационных системах (далее - ИС) Областного государственного бюджетного учреждения дополнительного профессионального образования «Рязанский институт развития образования» (ОГБУ ДПО «РИРО») – далее институт, регламентирует порядок обращения с криптосредствами в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты информации.

1.2 Настоящая Инструкция подготовлена 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», утв. руководством 8 Центра ФСБ России от 21 февраля 2008 г. № 149/6/6-622 (далее – Типовые требования).

1.3 Под криптосредством в настоящей Инструкции понимается шифровальное (криптографическое) средство, предназначенное для защиты информации.

1.4 К криптосредствам (шифровальным, криптографическим средствам) относятся:

1.4.1 Средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

1.4.2 Средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.

1.4.3 Средства электронной цифровой подписи – аппаратные, программные и аппаратно–программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи.

1.4.4 Средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций.

1.4.5 Средства изготовления ключевых документов (независимо от вида носителя ключевой информации).

1.4.6 Ключевые документы (независимо от вида носителя ключевой информации).

1.5 В настоящей Инструкции используются следующие понятия и определения:

1.5.1 Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

1.5.2 Доступ к информации - возможность получения информации и ее использования.

1.5.3 Закрытый ключ – криптоключ, который хранится пользователем системы в тайне.

1.5.4 Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.5.5 Ключевой документ - физический носитель определенной структуры, содержащий криптоключи.

1.5.6 Компрометация криптоключа - утрата доверия к тому, что используемые криптоключи обеспечивают безопасность информации.

1.5.7 Контролируемая зона - пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

1.5.8 Криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

1.5.9 Модель нарушителя - предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

1.5.10 Модель угроз - перечень возможных угроз.

1.5.11 Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.5.12 Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.5.13 Персональные данные - любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

1.5.14 Пользователь криптосредства - лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

1.5.15 Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

1.5.16 Режимные помещения - помещения, где установлены криптосредства или хранятся ключевые документы к ним.

1.5.17 Средство защиты информации - техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

1.6 Для обеспечения безопасности персональных данных при их обработке в институте должны использоваться сертифицированные в системе сертификации ФСБ России криптосредства (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации).

1.7 Класс криптосредства определяется в соответствии с «Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утв. руководством 8 Центра ФСБ России от 21 февраля 2008 г. № 149/54-144.

2 Организационная структура

2.1 Безопасность обработки персональных данных (далее - ПДн) в институте с использованием криптосредств организует и обеспечивает Администратор ИБ ИС.

3 Обязанности пользователей криптосредств

3.1 Пользователи криптосредств допускаются к работе с ними только после ознакомления под роспись с настоящей Инструкцией, Типовыми требованиями, другими документами, регламентирующими организацию и обеспечение безопасности ПДн при их обработке в ИС.

3.2 При наличии двух и более пользователей криптосредств обязанности между ними должны быть распределены с учетом персональной ответственности за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

3.3 Ответственный за эксплуатацию СКЗИ обязан:

3.3.1 Осуществлять поэкземплярный учет используемых оператором криптосредств, эксплуатационной и технической документации к ним.

3.3.2 Осуществлять контроль за соблюдением условий использования криптосредств, установленных эксплуатационной и технической документацией на СКЗИ и настоящей инструкцией.

3.3.3 Осуществлять учет Пользователей криптосредств.

3.3.4 Надежно хранить эксплуатационную и техническую документацию к криптосредствам, ключевые документы, носители дистрибутивов криптосредств, бумажные и машинные носители ПДн.

3.3.5 Проводить расследования и составлять заключения по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации.

3.3.6 Осуществлять разработку и принимать меры по предотвращению возможных негативных последствий нарушений.

3.4 Пользователи криптосредств обязаны:

3.4.1 Не нарушать конфиденциальность закрытых ключей.

3.4.2 Не допускать снятие копий с ключевых документов, содержащих закрытые ключи.

3.4.3 Не допускать вывод закрытых ключей на дисплей (монитор) ПЭВМ или принтер.

3.4.4 Не допускать записи на ключевой документ посторонней информации.

3.4.5 Не допускать установки ключевых документов в другие ПЭВМ.

3.4.6 Обеспечить конфиденциальность информации о криптосредствах, других мерах защиты.

3.4.7 Не нарушать конфиденциальность защищаемых ПДн.

3.4.8 Точно соблюдать требования к обеспечению безопасности ПДн, требования к обеспечению безопасности криптосредств и ключевых документов к ним.

3.4.9 Хранить ключевые документы к криптосредствам в защищаемых хранилищах.

3.4.10 Сдавать ключевые документы к криптосредствам при увольнении или отстранении от исполнения обязанностей.

3.4.11 Своевременно выявлять и сообщать Ответственному за эксплуатацию СКЗИ и Ответственному за организацию обработки ПДн в ИС о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним, защищаемых ПДн.

3.4.12 Немедленно уведомлять Ответственного за эксплуатацию СКЗИ и Ответственного за организацию обработки ПДн в ИС и принимать меры по предупреждению нарушения конфиденциальности защищаемых ПДн при утрате или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей, удостоверений, пропусков, при других фактах, которые могут привести к компрометации закрытых ключей, снижению уровня защищенности ПДн.

4 Учет ключевых документов

4.1 Ключевые документы подлежат поэкземплярному учету. Единицей поэкземплярного учета ключевых документов считается ключевой носитель информации.

4.2 Все экземпляры ключевых документов выдаются пользователям криптосредств под роспись в соответствующем журнале поэкземплярного учета.

4.3 Передача ключевых документов допускается только между пользователями криптосредств и Ответственным за эксплуатацию СКЗИ под роспись в соответствующем Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов. Аналогичная передача между пользователями криптосредств осуществляется с санкции Ответственного за эксплуатацию СКЗИ.

4.4 Для исключения компрометации ключевых документов, на период отсутствия пользователя и в нерабочее время, ключевые документы убираются в защищенные хранилища (сейфы, железные ящики), которые, в свою очередь, закрываются на ключ и опечатываются.

4.5 Учет эксплуатационной и технической документации к криптосредствам:

4.5.1 Эксплуатационная и техническая документация к криптосредствам подлежит поэкземплярному учету.

4.5.2 Все экземпляры эксплуатационной и технической документации к криптосредствам выдаются пользователям криптосредств под роспись.

4.5.3 Передача эксплуатационной и технической документации к криптосредствам допускается только между пользователями криптосредств и Ответственным за эксплуатацию СКЗИ под роспись. Аналогичная передача между пользователями криптосредств осуществляется с санкции Ответственного за эксплуатацию СКЗИ.

4.6 Распространение ключевых документов:

4.6.1 Ключевые документы получаются лично владельцем криптографического ключа в удостоверяющем центре.

4.7 Плановая смена ключевых документов:

4.7.1 Заказ на изготовление очередных ключевых документов, их изготовление и получение пользователем производится заблаговременно для своевременной замены действующих ключевых документов.

4.8 Внеплановая смена ключевых документов:

4.8.1 Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи немедленно выводятся из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам.

4.9 Уничтожение ключевых документов:

4.9.1 Ключевые документы с неиспользованными или выведенными из действия криптоключами (исходной ключевой информацией) возвращаются Ответственному за эксплуатацию СКЗИ, или по его указанию уничтожаются на месте пользователями криптосредств.

4.9.2 Уничтожение ключевых документов производится путем стирания (разрушения) криптоключей без повреждения ключевого документа.

4.9.3 Бумажные и прочие сгораемые ключевые документы уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

4.9.4 Ключевые документы уничтожаются в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. Если срок уничтожения

эксплуатационной и технической документацией не установлен, то ключевые документы уничтожаются не позднее 10 суток после вывода их из действия (окончания срока действия).

4.9.5 Пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) ключевые документы. После уничтожения пользователи криптосредств уведомляют об этом Администратора ИБ ИС.

4.10 Уничтожение эксплуатационной и технической документации к криптосредствам:

4.10.1 Эксплуатационная и техническая документация к криптосредствам уничтожается путем сжигания или с помощью любых бумагорезательных машин.

5 Техническое обслуживание криптосредств

5.1 Техническое обслуживание криптосредств, а также другого оборудования, функционирующего с криптосредствами, смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

5.2 На время отсутствия пользователей криптосредства, а также другое оборудование, функционирующее с криптосредствами, при наличии технической возможности, выключается, отключается от линии связи и убирается в опечатываемые хранилища. В противном случае необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

6 Опечатывание аппаратных средств

6.1 Системные блоки АРМ, на которых установлены криптосредства, должны оборудоваться средствами контроля за их вскрытием (опечатываются, опломбируются). Место опечатывания (опломбирования) системного блока должно быть таким, чтобы его можно было визуально контролировать.

7 Организация режима помещений

7.1 Охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним (далее - режимные помещения), должны обеспечивать сохранность ПДн, криптосредств и ключевых документов к ним, исключать возможность неконтролируемого проникновения или пребывания в режимных помещениях посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

7.2 При оборудовании режимных помещений должны выполняться требования к размещению, монтажу криптосредств, а также другого оборудования, функционирующего с криптосредствами.

7.3 Перечисленные в настоящей Инструкции требования к режимным помещениям могут не предъявляться, если это предусмотрено правилами пользования криптосредствами, согласованными с ФСБ России.

7.4 Режимные помещения выделяются с учетом размеров контролируемых зон. 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 режимные помещения посторонних лиц, оборудуются металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

7.5 Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливается ответственным за организацию обработки ПДн в ИС.

7.6 Двери режимных помещений должны закрываться на замок и могут открываться только для санкционированного прохода сотрудников и посетителей.

7.7 Режимные помещения должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации.

8 Порядок доступа к хранилищам

8.1 Эксплуатация хранилищ:

8.1.1 Пользователи криптосредств хранят, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в металлических хранилищах (ящиках, шкафах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

8.1.2 Металлические хранилища должны быть оборудованы внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин.

8.1.3 Должно быть предусмотрено раздельное безопасное хранение пользователями криптосредств действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

8.2 При необходимости доступа к содержимому хранилища сотрудник, ответственный за данное хранилище, проверяет целостность хранилища, открывает механический замок хранилища с использованием ключа.

8.3 По окончании работы сотрудник закрывает и опечатывает хранилище, за которое он ответственен.

8.4 Печати, предназначенные для опечатывания хранилищ, должны находиться у сотрудников, ответственных за данные хранилища.

8.5 Порядок предоставления сотрудникам ключей для доступа к хранилищам:

8.5.1 Рабочий ключ от хранилища предоставляется сотруднику, ответственному за данное хранилище, под роспись в соответствующем журнале ответственным за эксплуатацию хранилищ.

8.5.2 Запасные экземпляры ключей от хранилищ хранятся в сейфе (хранилище) ответственного за эксплуатацию хранилищ.

8.5.3 Запасные экземпляры ключей от сейфа ответственного за эксплуатацию хранилищ передаются в опечатанном пенале под роспись в соответствующем журнале.

8.5.4 Ключи от хранилища не должны предоставляться сотрудникам, не ответственным за данные хранилища.

8.5.5 Изготовлять ключи от механического замка хранилищ имеет право только ответственный за эксплуатацию хранилищ.

8.5.6 Ключи от механических замков хранилищ должны быть пронумерованы, учтены в соответствующем журнале.

8.5.7 При увольнении сотрудника, либо при назначении другого лица ответственным за хранилище данного сотрудника, сотрудник обязан сдать имеющиеся у него ключи от механического замка хранилища ответственному за эксплуатацию хранилищ.

8.5.8 Сотрудникам запрещено передавать кому-либо ключи от хранилищ кроме как в случаях, предусмотренных настоящей Инструкцией.

8.6 Действия при несанкционированном проникновении или утрате ключей от хранилища:

8.6.1 При утрате ключа от хранилища замок данного хранилища 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. Об утрате ключа сотрудник должен немедленно оповестить Ответственного за хранилища и ключи от них. Порядок хранения документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает Ответственный за хранилища и ключи от них.

8.6.2 При обнаружении признаков, указывающих на возможное несанкционированное проникновение в хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за эксплуатацию хранилищ. Ответственный за хранилища и ключи

от них должен оценить возможность компрометации, хищения, подмены, порчи хранящихся документов и технических средств, составить акт и принять, при необходимости, меры к локализации последствий.

9 Контроль безопасности криптосредств

9.1 Текущий контроль за организацией и обеспечением функционирования криптосредств возлагается на Администратора ИБ ИС в пределах его полномочий.

10 Ответственность за нарушение требований

10.1 Пользователи криптосредств несут персональную ответственность за сохранность полученных криптосредств, эксплуатационной и технической документации к криптосредствам, ключевых документов, за соблюдение положений настоящей Инструкции.

11.1 Администратор ИБ ИС несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности обработки ПДн с использованием криптосредств лицензионным требованиям и условиям эксплуатационной и технической документации к криптосредствам, а также настоящей Инструкции.

Директор по ПРСО [signature] О.В. Генералова

Согласовано: юрист [signature] Л.И. [illegible]