АГЕНТСТВО ПО РЕГУЛИРОВАНИЮ ЦЕН И ТАРИФОВ УЛЬЯНОВСКОЙ ОБЛАСТИ

П Р И К А З

6 октября 2022г № 80-П

Экз. №_____

г. Ульяновск

Об утверждении инструкции по обращению со средствами криптографической защиты информации

В связи с использованием средств криптографической защиты информации в Агентстве по регулированию цен и тарифов Ульяновской области, п р и к а з ы в а ю:

1. Утвердить:

1) инструкцию по обращению со средствами криптографической защиты информации в Агентстве по регулированию цен и тарифов Ульяновской области (приложение № 1);

2) форму перечня сотрудников, допущенных к работе со средствами криптографической защиты информации (приложение № 2);

3) форму журнала поэкземплярного учёта средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов (приложение № 3);

4) форму журнала регистрации, учёта и выдачи средств криптографической защиты информации (приложение № 4).

2. Настоящий приказ вступает в силу на следующий день после для его официального опубликования.

Руководитель А.В.Филин

0000854

ПРИЛОЖЕНИЕ № 1

к приказу Агентства
по регулированию цен и тарифов
Ульяновской области
от 6 октября 2022 г. № 80-П

ИНСТРУКЦИЯ
по обращению со средствами криптографической защиты информации в Агентстве по регулированию цен и тарифов Ульяновской области

1. Общие положения

1.1. Инструкция по обращению со средствами криптографической защиты информации (далее – Инструкция) в Агентстве по регулированию цен и тарифов Ульяновской области (далее – Агентство) регламентирует порядок обращения, получения, хранения, доставки, передачи, тестирования средств криптографической защиты информации (далее - СКЗИ) в целях защиты информации.

1.2. Настоящая Инструкция подготовлена в соответствии с приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации 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».

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

1.4. К СКЗИ относятся:

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 её обработке и хранении;

2) средства электронной подписи – аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием ключа электронной подписи, подтверждение с использованием ключа проверки электронной подписи подлинности электронной подписи, создание ключей электронной подписи и ключей проверки электронной подписи;

3) средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части

преобразования путём ручных операций или с использованием автоматизированных средств на основе таких операций;

4) средства изготовления ключевых документов (независимо от вида носителя ключевой информации);

5) ключевые документы (независимо от вида носителя ключевой информации).

1.5. В настоящей Инструкции используются следующие понятия и определения:

1) доступ к информации - возможность получения информации и её использования;

2) ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;

3) ключевой документ - физический носитель определенной структуры, содержащий криптоключи;

4) компрометация криптоключа - утрата доверия к тому, что используемые криптоключи обеспечивают безопасность информации;

5) криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;

6) пользователь СКЗИ - лицо, участвующее в эксплуатации СКЗИ или использующее результаты его функционирования;

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

1.6. Для обеспечения безопасности информации должны использоваться сертифицированные в системе сертификации Федеральной службы безопасности Российской Федерации СКЗИ (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации).

2. Организационная структура

Безопасность обработки информации с использованием СКЗИ организует и обеспечивает администратор информационной безопасности (далее – ответственный за эксплуатацию СКЗИ).

3. Обязанности пользователей СКЗИ

3.1. Пользователи СКЗИ допускаются к работе с ними только после ознакомления под роспись с настоящей Инструкцией и другими документами, регламентирующими организацию и обеспечение защиты информации в Агентстве (приложение к настоящей Инструкции).

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

3.3. Ответственный за эксплуатацию СКЗИ обязан:

1) осуществлять поэкземплярный учёт используемых в Агентстве СКЗИ, эксплуатационной и технической документации к ним;

2) осуществлять контроль за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией на СКЗИ и настоящей инструкцией;

3) осуществлять учёт пользователей СКЗИ;

4) надёжно хранить эксплуатационную и техническую документацию к СКЗИ, ключевые документы, носители дистрибутивов СКЗИ;

5) проводить расследования и составлять заключения по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации;

6) осуществлять разработку и принимать меры по предотвращению возможных негативных последствий нарушений.

3.4. Пользователи СКЗИ обязаны:

1) не нарушать конфиденциальность ключей электронной подписи;

2) не допускать снятие копий с ключевых документов, содержащих ключи электронной подписи;

3) не допускать вывод ключей электронной подписи на дисплей (монитор) ПЭВМ или принтер;

4) не допускать записи на ключевой документ посторонней информации;

5) не допускать установки ключевых документов в другие ПЭВМ;

6) обеспечить конфиденциальность информации о СКЗИ, других мерах защиты;

7) точно соблюдать требования к обеспечению безопасности информации, требования к обеспечению безопасности СКЗИ и ключевых документов к ним.

8) хранить ключевые документы к СКЗИ в защищаемых хранилищах;

9) сдавать ключевые документы к СКЗИ при увольнении или отстранении от исполнения обязанностей;

10) своевременно выявлять и сообщать ответственному за эксплуатацию СКЗИ о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

11) немедленно уведомлять ответственного за эксплуатацию СКЗИ и принимать меры по предупреждению нарушения конфиденциальности информации при утрате или недостаче СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей, удостоверений, пропусков, при других фактах, которые могут привести к компрометации ключей электронной подписи.

4. Учёт ключевых документов

4.1. Ключевые документы подлежат поэкземплярному учёту. Единицей поэкземплярного учёта ключевых документов считается ключевой носитель информации.

4.2. Все экземпляры ключевых документов выдаются пользователям СКЗИ под роспись в соответствующем журнале поэкземплярного учёта.

4.3. Передача ключевых документов допускается только между пользователями СКЗИ и ответственным за эксплуатацию СКЗИ под роспись в соответствующем Журнале поэкземплярного учёта средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов. Аналогичная передача между пользователями СКЗИ 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. Учёт эксплуатационной и технической документации к СКЗИ:

1) эксплуатационная и техническая документация к СКЗИ подлежит поэкземплярному учёту;

2) все экземпляры эксплуатационной и технической документации к СКЗИ выдаются пользователям СКЗИ под роспись;

3) передача эксплуатационной и технической документации к СКЗИ допускается только между пользователями СКЗИ и ответственным за эксплуатацию СКЗИ под роспись. Аналогичная передача между пользователями криптосредств осуществляется с санкции ответственного за эксплуатацию СКЗИ.

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

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

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

4.9. 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 СКЗИ.

4.9.1. Уничтожение ключевых документов производится путём стирания (разрушения) криптоключей без повреждения ключевого документа.

4.9.2. Бумажные и прочие сгораемые ключевые документы уничтожаются путём сжигания или с помощью любых бумагорезательных машин.

4.9.3. Ключевые документы уничтожаются в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. 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).

4.9.4. Пользователям СКЗИ разрешается уничтожать только использованные непосредственно ими (предназначенные для них) ключевые документы. После уничтожения пользователи СКЗИ уведомляют об этом администратора информационной безопасности.

4.10. Эксплуатационная и техническая документация к СКЗИ уничтожается путём сжигания или с помощью любых бумагорезательных машин.

5. Техническое обслуживание СКЗИ

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

5.2. На время отсутствия пользователей СКЗИ, а также другое оборудование, функционирующее с СКЗИ, 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 СКЗИ посторонними лицами.

6. Опечатывание аппаратных средств

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

7. Порядок доступа к хранилищам

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

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

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

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

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

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

7.5. Порядок предоставления сотрудникам ключей для доступа к хранилищам:

1) рабочий ключ от хранилища предоставляется сотруднику, ответственному за данное хранилище, под роспись в соответствующем журнале ответственным за эксплуатацию хранилищ;

2) запасные экземпляры ключей от хранилищ хранятся в сейфе (хранилище) ответственного за эксплуатацию хранилищ;

3) запасные экземпляры ключей от сейфа ответственного за эксплуатацию хранилищ передаются в опечатанном пенале под роспись в соответствующем журнале;

4) ключи от хранилища не должны предоставляться сотрудникам, не ответственным за данные хранилища;

5) изготовлять ключи от механического замка хранилищ имеет право только ответственный за эксплуатацию хранилищ;

6) ключи от механических замков хранилищ должны быть пронумерованы, учтены в соответствующем журнале;

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

7.6. Действия при несанкционированном проникновении или утрате ключей от хранилища:

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;

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.

8. Контроль безопасности криптосредств

Текущий контроль за организацией и обеспечением функционирования СКЗИ возлагается на администратора информационной безопасности в пределах его полномочий.

9. Ответственность за нарушение требований

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

9.2. Администратор информационной безопасности несёт ответственность за соответствие проводимых им мероприятий по организации защиты информации с использованием СКЗИ, лицензионным требованиям и условиям эксплуатационной и технической документации к СКЗИ, а также настоящей Инструкции.

Приложение к Инструкции
по обращению со средствами
криптографической защиты
информации в Агентстве
по регулированию цен и тарифов
Ульяновской области

Лист ознакомления с Инструкцией
по обращению со средствами криптографической защиты информации
в Агентстве по регулированию цен и тарифов Ульяновской области
№ _____ от «___» _____ 202__ г.

№ п/п	Должность	Фамилия, Имя, Отчество	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				

ПРИЛОЖЕНИЕ № 2

к приказу Агентства
по регулированию цен и тарифов
Ульяновской области
от 6 октября 2022 г. № 80-Л

ПЕРЕЧЕНЬ
сотрудников, допущенных к работе со средствами криптографической защиты информации в Агентстве по регулированию цен и тарифов Ульяновской области

№ п/п	Ф.И.О.	Должность	Включён в перечень на основании	Исключён из перечня на основании	Примечание
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					

ПРИЛОЖЕНИЕ № 3

к приказу Агентства
по регулированию цен и тарифов
Ульяновской области
от 6 октября 2022 г. № 80-П

ЖУРНАЛ №____
поэкземплярного учёта средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

Начат «___» _____ 202__ г. На ____ листах
Окончен «___» _____ 202__ г.

_____ _____
(ФИО ответственного лица за ведение журнала) подпись

№ 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 рассылке (передаче)		
				От кого получены или Ф.И.О. сотрудника органа криптографической защиты, изготовившего ключевые документы	Дата и номер сопроводительного письма или дата изготовления ключевых документов и расписка в изготовлении	Кому разосланы (переданы)	Дата и номер сопроводительного письма	Дата и номер подтверждения или расписка в получении
1	2	3	4	5	6	7	8	9

ПРИЛОЖЕНИЕ № 4

к приказу Агентства
по регулированию цен и тарифов
Ульяновской области
от 6 октября 2022 г. № 80-П

ЖУРНАЛ №____
регистрации, учёта и выдачи средств криптографической защиты информации
в Агентстве по регулированию цен и тарифов Ульяновской области

Начат «___» _____ 20___ г. На ____ листах
Окончен «___» _____ 20___ г.

_____ _____
(ФИО ответственного лица за ведение журнала) подпись

Регистрационный номер носителя информации	Дата регистрации	Название носителя информации	Ф.И.О. получившего носитель информации	Дата и время получения носителя информации	Подпись получившего носитель информации	Подпись администратора информационной безопасности	Дата и время сдачи носителя информации	Подпись сдавшего носитель информации	Подпись администратора информационной безопасности	Примечание