**Приказ ФАПСИ от 13 июня 2001 г. №152 «Об утверждении Инструкции об организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»**

Документ состоит из 5 глав и 3-х приложений

1. **Общие положения**

Инструкция определяет единый на территории РФ порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных ФАПСИ средств криптографической защиты (шифровальных средств).

Не применяется в учреждениях РФ за границей.

1. **Организация и обеспечение безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.**

Безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации **в сетях конфиденциальной связи**\* организуют и обеспечивают **операторы конфиденциальной связи**\*\*

\***Сети конфиденциальной связи** - сети связи, предназначенные для передачи конфиденциальной информации.

**\*\*Операторы конфиденциальной связи** - операторы связи, предоставляющие на основании лицензии ФАПСИ услуги конфиденциальной связи с использованием СКЗИ.

**СКЗИ** (**средство криптографической защиты информации**) — **это** программа или устройство, которое шифрует документы и генерирует электронную подпись (ЭП). Все операции производятся с помощью ключа электронной подписи, который невозможно подобрать вручную, так как он представляет собой сложный набор символов.

Лицензиаты ФАПСИ организуют и обеспечивают защиту информации для лиц не имеющих лицензию на договорной основе или по указанию вышестоящей организации.

Лицензиаты ФАПСИ несут ответственность за соответствие проводимых ими мероприятий по обеспечению безопасности.

Для осуществлений мероприятий по обеспечению безопасности лицензиат ФАПСИ создает один или несколько **органов криптографической защиты**\*.

\***Органом криптографической защиты** может быть организация, структурное подразделение организации - лицензиата ФАПСИ, обладателя конфиденциальной информации. Функции органа криптографической защиты могут быть возложены на физическое лицо.

Орган криптографической защиты осуществляет:

* проверку готовности обладателей конфиденциальной информации к самостоятельному использованию СКЗИ
* разработку мероприятий по обеспечению функционирования и безопасности применяемых СКЗИ
* обучение лиц, использующих СКЗИ, правилам работы с ними
* поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним
* учет обслуживаемых обладателей конфиденциальной информации

К выполнению обязанностей сотрудников органов криптографической защиты лицензиатами ФАПСИ допускаются лица, имеющие необходимый уровень квалификации для обеспечения защиты конфиденциальной информации, также им необходимо ознакомиться с инструкцией под расписку.

Пользователи СКЗИ обязаны:

* не разглашать конфиденциальную информацию, к которой они допущены, рубежи ее защиты, в том числе сведения о криптоключах;
* соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
* сообщать в орган криптографической защиты о ставших им 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 порядком;
* немедленно уведомлять орган криптографической защиты 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 защищаемых сведений конфиденциального характера.

Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения

1. **Порядок обращения к СКЗИ и криптоключам к ним. Мероприятия при компрометации криптоключей.**

Под компрометацией криптоключей понимается хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

Документы предназначенные для обеспечения безопасности не должны содержать сведения, составляющие государственную тайну

Для обеспечения безопасности следует использовать СКЗИ, позволяющие реализовать принцип абонентского шифрования и предусматривающие запись криптоключей на электронные ключевые носители многократного (долговременного) использования

Все экземпляры с необходимой документацией выдаются под расписку.

Передача может осуществляться только между пользователями СКЗИ и сотрудниками органа криптографической защиты.

При пересылке необходимо качественно упаковать документы, подготовив сопроводительное письмо. При обнаружении бракованных ключевых документов возвратить изготовителю до устранения причин произошедшего.

Уничтожение исходной информации может производиться путем физического уничтожения ключевого носителя или путем стирания исходной информации.

Ключевые документы должны быть уничтожены в сроки, указанные в документации.

1. **Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним.**

Спецпомещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Окна спецпомещений необходимо оборудовать металлическими решетками.

Размещение, специальное оборудование, охрана и организация режима в спецпомещениях органов криптографической защиты должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

Лицензиат ФАПСИ устанавливает режим охраны спецпомещений.

По окончанию рабочего дня все спецпомещения должны быть закрыты, хранилища опечатаны. Ключи отдаются посту охраны под расписку. При утрате ключа, необходимо заменить замок в спецпомещение.

1. **Контроль за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.**

Контроль за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации осуществляют **федеральные органы правительственной связи и информации\***

\*Под федеральными органами правительственной связи и информации в настоящей Инструкции понимаются главные управления ФАПСИ, управления ФАПСИ в федеральных округах, региональные управления правительственной связи и информации, центры правительственной связи.

В ходе государственного контроля изучаются и оцениваются:

* организация безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации;
* достигнутый уровень криптографической защиты конфиденциальной информации;
* условия использования СКЗИ.

Сроки и периодичность государственного контроля определяет ФАПСИ. По результатам государственного контроля составляется подробный или краткий акт, справка. С актом проверки (справкой) под расписку должно быть ознакомлено руководство проверяемых лиц.

Если в использовании СКЗИ обнаружены недостатки, то лицензиаты ФАПСИ, обладатели конфиденциальной информации обязаны принять безотлагательные меры к устранению вскрытых проверкой недостатков и выполнению рекомендаций, изложенных в акте проверки.

Если в использовании СКЗИ выявлены серьезные нарушения, из-за чего становится реальной утечка конфиденциальной информации, безопасность которой обеспечивается с использованием СКЗИ, то федеральные органы правительственной связи и информации, лицензиаты ФАПСИ вправе дать указание о немедленном прекращении использования СКЗИ до устранения причин выявленных нарушений.

Обладатель конфиденциальной информации вправе обратиться в федеральные органы правительственной связи и информации с просьбой о проведении на договорной основе государственного контроля с целью оценки достаточности и обоснованности принимаемых лицензиатом ФАПСИ мер защиты его конфиденциальной информации.