Особенности использования СКЗИ для защиты ПДн в государственных и муниципальных органах

Сидоров Михаил Александрович

Заместитель директора ООО «Просистем»

О нормативно-методических документах, действующих в области обеспечения безопасности ПДн

В настоящее время в области обеспечения безопасности персональных данных действуют следующие нормативно-методические документы ФСБ России:

1. Приказ ФСБ от 10 июля 2014 года № 378;
2. Приказ ФСБ России от 9 февраля 2005 года № 66;
3. Инструкция, утвержденная приказом ФАПСИ от 13 июня 2001 года № 152;
4. Методические рекомендации, утвержденные руководством 8 Центра ФСБ России (№ 149/7/2/6-432 от 31.03.2015)

Почему необходимо использовать СКЗИ?

Использование СКЗИ для обеспечения безопасности персональных данных необходимо в следующих случаях:

- если персональные данные подлежат криптографической защите в соответствии с законодательством Российской Федерации;
- если в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ;
- решение о необходимости криптографической защиты персональных данных принято конкретным оператором на основании технико-экономического сравнения альтернативных вариантов обеспечения требуемых характеристик безопасности информации, содержащей, в том числе, персональные данные.

Почему необходимо использовать СКЗИ?

К случаям, когда угрозы могут быть нейтрализованы только с помощью СКЗИ, относятся:

- передача персональных данных по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче персональных данных по информационно-телекоммуникационным сетям общего пользования);
- хранение персональных данных на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов.

Порядок эксплуатации СКЗИ

- СКЗИ эксплуатируются в соответствии с правилами пользования ими;
- СКЗИ, находящиеся в эксплуатации, должны подвергаться контрольным тематическим исследованиям, конкретные сроки проведения которых определяются заказчиком СКЗИ по согласованию с разработчиком СКЗИ, специализированной организацией и ФСБ России;
- СКЗИ и их опытные образцы **подлежат поэкземплярному учету** с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов (условных наименований) и регистрационных номеров поэкземплярного учета СКЗИ и их опытных образцов определяет ФСБ России **(см. Приложение 1 к Инструкции ФАПСИ от 13 июня 2001 г. N 152)**
- Организация поэкземплярного учета используемых СКЗИ возлагается на заказчика СКЗИ.

Участники эксплуатации СКЗИ

- **Органом криптографической защиты (ОКЗ)** может быть организация, структурное подразделение организации - лицензиата ФАПСИ, обладателя конфиденциальной информации. Функции органа криптографической защиты могут быть возложены **на физическое лицо;**
- Обязанности, возлагаемые на сотрудников ОКЗ, могут выполняться штатными сотрудниками или сотрудниками других структурных подразделений, привлекаемыми к такой работе по совместительству;
- К выполнению обязанностей сотрудников ОКЗ лицензиатами ФАПСИ допускаются лица, имеющие **необходимый уровень квалификации** для обеспечения защиты конфиденциальной информации с использованием конкретного вида (типа) СКЗИ;
- Лиц, оформляемых на работу в ОКЗ, следует ознакомить с настоящей Инструкцией под расписку;
- Необходимо разработать инструкции сотрудникам ОКЗ, определяющую их функциональные обязанности.

Обязанности органа криптографической защиты

Орган криптографической защиты осуществляет:

- Проверку готовности обладателей конфиденциальной информации к самостоятельному использованию СКЗИ и составление заключений о возможности эксплуатации СКЗИ;
- Разработку мероприятий по обеспечению функционирования и безопасности применяемых СКЗИ в соответствии с документацией;
- Обучение лиц, использующих СКЗИ, правилам работы с ними;
- Поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним **(см. Приложение 1 к Инструкции ФАПСИ от 13 июня 2001 г. N 152)**;
- Учет обслуживаемых обладателей конфиденциальной информации, а также физических лиц, непосредственно допущенных к работе с СКЗИ;
- Подачу заявлений на изготовление ключевых документов или исходной ключевой информации. Изготовление из исходной ключевой информации ключевых документов, их распределение, рассылку и учет;
- Контроль за соблюдением условий использования СКЗИ;
- Расследование и составление заключений по фактам нарушения условий использования СКЗИ;
- Разработку схемы организации криптографической защиты конфиденциальной информации.

Обязанности органа криптографической защиты

Орган криптографической защиты осуществляет:

- Подготовку перечня помещений, предназначенных для обработки ПДн с использованием СКЗИ;
- Подготовку перечня лиц (пользователей), допущенных к обработке ПДн с использованием СКЗИ;
- Разработку правил доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях;
- Заводят и ведут на каждого пользователя СКЗИ лицевой счет, в котором регистрируют числящиеся за ним СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы;
- Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники соответствующего ОКЗ. Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе с СКЗИ, является **заключение**, составленное комиссией соответствующего ОКЗ **на основании принятых от этих лиц зачетов по программе обучения.**

Обязанности пользователя СКЗИ

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 ОКЗ о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документов к ним;
- Сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- Немедленно уведомлять ОКЗ 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, а также о причинах и условиях возможной утечки таких сведений;

Уничтожение СКЗИ

- Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования);
- Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ, но **не позднее 10 суток** после вывода их из действия (окончания срока действия);
- Ключевые документы уничтожаются либо пользователями СКЗИ, либо сотрудниками ОКЗ под расписку в соответствующих **журналах поэкземплярного учета**, а уничтожение большого объема ключевых документов может быть оформлено **актом**;
- Не реже одного раза в год пользователи СКЗИ должны направлять в ОКЗ письменные отчеты об уничтоженных ключевых документах;
- Уничтожение по акту производит комиссия в составе не менее двух человек из числа сотрудников ОКЗ.

Защита помещений ОКЗ

- Двери спецпомещений ОКЗ должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей;
- Ключи от входных дверей нумеруют, учитывают и выдают сотрудникам ОКЗ под расписку в журнале учета хранилищ;
- Дубликаты ключей от входных дверей таких спецпомещений следует хранить в сейфе руководителя ОКЗ. Хранение дубликатов ключей вне помещений ОКЗ не допускается;
- Спецпомещения ОКЗ, как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации **(либо опечатываться)**;
- ОКЗ должен иметь необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у сотрудника, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в сейфе руководителя ОКЗ.

Защита помещений ОКЗ

- По окончании рабочего дня спецпомещения ОКЗ и установленные в них хранилища должны быть закрыты, хранилища опечатаны;
- Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в соответствующем журнале руководителю ОКЗ или лицу, им уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище;
- Ключи от спецпомещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ ОКЗ, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службе охраны или дежурному по организации одновременно с передачей под охрану самих спецпомещений.
- Печати, предназначенные для опечатывания хранилищ, должны находиться у сотрудников ОКЗ, ответственных за эти хранилища.

Защита помещений пользователей СКЗИ

- Режим охраны спецпомещений пользователей СКЗИ, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает обладатель конфиденциальной информации по согласованию с соответствующим ОКЗ;
- В спецпомещениях пользователей СКЗИ для хранения выданных им ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин;
- Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ;
- Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ **должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы)**;
- При наличии технической возможности на время отсутствия пользователей СКЗИ указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

Перечень организационно-распорядительных документов по СКЗИ

- Приказ о назначении ответственного пользователя криптосредств;
- Инструкция ответственного пользователя криптосредств;
- Инструкция пользователя криптосредств;
- Порядок обращения с криптосредствами, а также порядок восстановления связи в случае компрометации действующих ключей к криптосредствам
- Перечень сотрудников, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационных системах персональных данных (пользователи криптосредств);
- Перечень помещений, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств;
- Перечень лиц, имеющих доступ в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств;
- Перечень мест хранения криптосредств, носителей ключевой, аутентифицирующей и парольной информации криптосредств;

Перечень организационно-распорядительных документов по СКЗИ

- Порядок доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств;
- Лицевой счет пользователя криптосредств;
- Акт об уничтожении криптографических ключей и ключевых документов;
- Журнал учета и выдачи носителей с ключевой информацией;
- Журнал обучения пользователей правилам работы с криптосредствами.

Спасибо за внимание!

Сидоров Михаил Александрович
ООО «Просистем»

E-mail: sm@p-system.ru

тел. 8 (3842) 56-14-24, 56-15-75