ТРЕБОВАНИЯ
по размещению СКЗИ в учреждениях (организациях)

Настоящие Требования разработаны в соответствии с «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» (введена Приказом ФАПСИ от 13.06.2001 № 152) и эксплуатационной документацией на используемые в учреждениях (организациях) средства криптографической защиты информации (далее – СКЗИ) и определяют основные требования по размещению СКЗИ.

1 Требования к размещению СКЗИ

Требования предъявляются к помещениям (спецпомещения), где установлен комплекс СКЗИ.

Размещение, специальное оборудование, охрана и организация режима в помещении, где установлен комплекс СКЗИ, должны обеспечивать:

- безопасность комплекса СКЗИ;
- невозможность доступа к комплексу СКЗИ лиц, не допущенных к работе с комплексом СКЗИ, к аппаратным и программным средствам комплекса СКЗИ, к просмотру процедур работы с комплексом СКЗИ;
- исключение кражи компонентов комплекса СКЗИ;
- исключение несанкционированного подключения устройств к комплексу СКЗИ.

Помещение должно быть обеспечено системами электроснабжения, обеспечивающими стабильное электропитание комплекса СКЗИ выделенное электроснабжение напряжением 220В с системой заземления TN-C-S/TN-S в соответствии с требованиями ПУЭ со свободной общей мощностью необходимой для подключения размещаемого оборудования. Качество электроснабжения должно соответствовать ГОСТ 32144-2013 за исключением требований к медленным изменениям напряжения. Медленные изменения напряжения питания должны находиться в диапазоне Uном +-5%. Температура и относительная влажность воздуха в помещении должны находиться в диапазонах от 0 °С до 40 °С и от 5 % до 90 % при 25 °С соответственно.

Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Двери помещений 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 под расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей таких помещений следует хранить в сейфе уполномоченного за размещение СКЗИ работника учреждения. Хранение дубликатов ключей вне помещений не допускается.

Окна помещений, расположенных на первых или последних этажах зданий необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения. Рядом с окнами помещений не должно быть пожарных лестниц, водосточных и других мест, откуда возможно проникновение в помещения посторонних лиц. Для предотвращения просмотра извне помещений их окна должны быть защищены.

В учреждении должен быть установлен режим круглосуточной охраны корпусов предприятия и помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время (обеспечение пропускного режима). Должен быть обеспечен контроль внешнего периметра и внутренних помещений. помещения, должны быть оснащены охранной и пожарной сигнализацией, связанной со службой охраны здания или дежурным по организации. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны. Исправность сигнализации периодически необходимо проверять уполномоченному за размещение СКЗИ работнику учреждения или по его поручению другому сотруднику этого учреждения совместно с представителем службы охраны или дежурным по организации с отметкой в соответствующих журналах.

По окончании рабочего дня помещения должны быть закрыты. Ключи от помещений должны быть сданы под расписку в соответствующем журнале службе охраны или дежурному по организации одновременно с передачей под охрану самих помещений. При утрате ключа от входной двери в помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением.

2 Требования к организации доступа к СКЗИ

Должны быть приняты меры по исключению несанкционированного доступа в помещение, в котором находится комплекс СКЗИ, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в указанном помещении.

Право доступа к компонентам комплекса СКЗИ предоставляется только ответственному от ПАО «Ростелеком» за эксплуатацию СКЗИ.

Персонал учреждения должен периодически визуально проводить контроль сохранности печатей (пломб) системных блоков комплекса СКЗИ.

3 Требования к порядку обслуживания и наладки СКЗИ

При возникновении нештатных ситуаций с комплексом СКЗИ уполномоченный за размещение СКЗИ работник учреждения направляет заявку в ПАО «Ростелеком», которая должна содержать в том числе следующие сведения:

- информация о заявителе (наименование и адрес учреждения);
- сведения о комплексе СКЗИ (модель, заводской номер);

- сведения о неисправности и/или необходимых работах.

Заявка подается по телефону или в электронной форме в ПАО «Ростелеком» по контактам, указанным в разделе 6.

Менеджер ПАО «Ростелеком» назначает на исполнение Заявки специалиста, ответственного от ПАО «Ростелеком» за эксплуатацию СКЗИ, сообщает заявителю о дате и времени прибытия специалиста и его контактные данные.

Техническое обслуживание комплекса СКЗИ осуществляется сотрудником ПАО «Ростелеком».

Выполнение работ подтверждается Актом выполненных работ.

4 Ограничения

После установки и эксплуатации СКЗИ запрещается:

- разглашать конфиденциальную информацию, связанную с применением СКЗИ (раздел 5);
- нарушать требования по охране и организации доступа к СКЗИ (разделы 1, 2);
- оставлять СКЗИ без контроля;
- осуществлять несанкционированное вскрытие СКЗИ;
- изымать из СКЗИ носители, передавать или производить их копирование;
- подключать, переключать или перекоммутировать с СКЗИ устройства, оборудование, кабели самостоятельно;
- вносить изменения в предустановленное на СКЗИ ПО или в состав аппаратных средств СКЗИ;
- самостоятельно производить администрирование (настройку, конфигурирование) СКЗИ;
- нарушать целостность пломб на СКЗИ или их мест установки;
- не исполнять/игнорировать указания ответственного от ПАО «Ростелеком» за эксплуатацию СКЗИ;
- скрывать, умалчивать или не уведомлять ответственного от ПАО «Ростелеком» за эксплуатацию СКЗИ о подозрениях или фактах нарушений условий функционирования (запретов), связанных с установкой и эксплуатацией СКЗИ, в том числе пропаже СКЗИ.

5 Перечень конфиденциальной информации

В целях обеспечения заданного уровня информационной безопасности запрещается распространение, в том числе обсуждение, с лицами не допущенными в установленном порядке конфиденциальной информации, связанной с применением СКЗИ.

К такой информации относится:

- Информация о месте размещения СКЗИ;

- Информация о подключаемых к СКЗИ каналах связи и линий электропитания;
- Информация об организованных мерах контроля доступа и защиты СКЗИ и его компонентам;
- Информация о лицах, допущенных в место/а размещения СКЗИ.

6 Обращения в ПАО «Ростелеком»

В целях обеспечения заданного уровня информационной безопасности обо всех подозрениях или фактах нарушений условий функционирования (запретов), связанных с установкой и эксплуатацией СКЗИ, в том числе пропаже СКЗИ, а также при обнаружении признаков, указывающих на возможное несанкционированное вскрытие системного блока комплекса СКЗИ или проникновение в помещение, в котором находится комплекс СКЗИ посторонних лиц, необходимо уведомлять ответственного от ПАО «Ростелеком» за эксплуатацию СКЗИ.

Контактные данные ответственного за эксплуатацию СКЗИ:

Телефон – 8 800 301 32 31 (круглосуточно)

Электронная почта – espd_ce@rt.ru

7 Ответственность и заключительные положения

В случае, разглашение конфиденциальной информации, бездействия или совершения противоправных действий в области защиты информации (в том числе нарушение настоящих требований) лица несут гражданско-правовую или иную ответственность в соответствии с действующим законодательством Российской Федерации.