Приложение
к приказу директора МБОУ СОШ № 30
г.Южно-Сахалинска
от 18.12.2014 № 435-ОД

Положение

о работе со средствами криптографической защиты информации в информационной системе персональных данных (ИСПДн) «Сетевой Город. Образование» (СГО)

1. Настоящее Положение разработано на основании статей следующих нормативных документов:
   - «Инструкция 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», утвержденная приказом ФАПСИ от 13.06.2001 №152;
   - «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом ФСБ от 9.02.2005 №66.
2. Контроль за соблюдением порядка работы со средствами криптографической защиты информации (СКЗИ) осуществляет Администратор безопасности информации.
3. Администратор безопасности информации допускается к работе с СКЗИ только после соответствующего обучения.
4. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним (далее — режимные помещения), должны обеспечивать сохранность конфиденциальной информации. СКЗИ и ключевых документов к ним.
5. При оборудовании режимных помещений должны выполняться требования к размещению, монтажу СКЗИ. а также другого оборудования, функционирующего с СКЗИ. указанные в эксплуатационных документах.
6. Режимные помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. 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. необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.
7. Размещение, специальное оборудование, охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц. а также просмотра посторонними лицами ведущихся там работ.
8. Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает Администратор безопасности информации по согласованию, при необходимости, с министром. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются.
9. Двери спецпомещений 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, имеющим право допуска в режимные помещения, под расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей таких помещений следует хранить в сейфе.

10. Для предотвращения просмотра извне режимных помещений их окна должны быть защищены.

11. Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей должно быть предусмотрено 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 ответственного пользователя СКЗИ. Дубликат ключа от хранилища ответственного пользователя СКЗИ в опечатанной упаковке должен быть передан на хранение оператору под расписку в соответствующем журнале.

12. По окончании рабочего дня режимное помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в соответствующем журнале Администратора безопасности информации или уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище.

13. Ключи от режимных помещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ режимного помещения, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службы охраны или дежурному по организации одновременно с передачей под охрану самих режимных помещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей СКЗИ. ответственных за эти хранилища.

14. При утрате ключа от хранилища или от входной двери в режимное помещение замок 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. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает Администратор безопасности информации.

15. В обычных условиях режимные помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями СКЗИ, ответственным пользователем СКЗИ или оператором.

16. Размещение и монтаж СКЗИ. а также другого оборудования, функционирующего с СКЗИ. в режимных помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц. не допущенных к работе с данными СКЗИ.

17. На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с Администратором безопасности информации необходимо предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами.

18. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним подлежат поэкземплярному учету в «Журнале поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним. ключевых документов в АИС «Сетевой Город. Образование» (СГО) МБОУ СОШ №30.

19. Если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криитокточи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ. то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале.

20. Неиспользованные или выведенные из действия ключевые документы подлежа! возвращению в орган криптографической защиты или по его указанию должны быть уничтожены на месте.

21. Уничтожение ключевой информации может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) исходной ключевой информации без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

22. Ключевую информацию, в отношении которой возникло подозрение в компрометации, необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ.