УТВЕРЖДАЮ:
И.о. директора ГБПОУ СПЦ №5
_____ Н.В. Колесникова
«02» декабря 2014г.

Положение
о работе со средствами криптографической защиты информации в информационной системе персональных данных «Сетевой город. Профессиональное образование» государственного бюджетного профессионального образовательного учреждения «Сахалинский политехнический центр №5»

1. Общие положения

Настоящее Положение о работе со средствами криптографической защиты информации в информационной системе персональных данных «Сетевой город. Профессиональное образование» (далее – Положение) разработано на основании:

- ✓ 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», утвержденной приказом ФАПСИ от 13.06.2001 №152;
- ✓ Положения «О разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденного приказом ФСБ от 9.02.2005 №66.

Контроль за соблюдением порядка работы со средствами криптографической защиты информации (далее - СКЗИ) осуществляет Администратор автоматизированной информационной системы «Сетевой город. Профессиональное образование» (далее – Администратор АИС СГПО).

Администратор АИС СГПО допускается к работе с СКЗИ только после соответствующего обучения.

2. Оборудование помещений для работы со СКЗИ

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.

При оборудовании режимных помещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ, указанные в эксплуатационных документах.

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.

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.

3. Организация работы в режимных помещениях

Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает Администратор АИС СГПО по согласованию, при необходимости, с директором ГБПОУ СПЦ №5. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются.

Двери режимных 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, имеющим право допуска в режимные помещения, под расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей таких помещений следует хранить в сейфе.

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

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.

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 Администратору АИС СГПО или уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище.

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.

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 АИС СГПО.

В обычных условиях режимные помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только лицами, ответственными за работу с СКЗИ.

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.

На время отсутствия лиц ответственных за работу с 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 Министерством образования Сахалинской области необходимо предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами.

Информация об используемых или хранимых СКЗИ, эксплуатационная и техническая документация к ним находится в Министерстве образования Сахалинской области.

О наличие ключевой информации, в отношении которой возникло подозрение в компрометации, необходимо немедленно оповестить лиц ответственных за безопасность информации в Министерстве образования Сахалинской области, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ.

Положение рассмотрено, согласовано
на заседании Общего собрания
Протокол от 24 ноября 2014г.