ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В СЭД

1. Рекомендации по организационному обеспечению безопасности СКЗИ:

- в организации Участника СЭД выделяются (определяются) должностные лица, ответственные за обеспечение безопасности информации и эксплуатацию СКЗИ;
- в организации Участника СЭД разрабатываются нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации СКЗИ;
- к работе с СКЗИ допускаются сотрудники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации СКЗИ.

2. Рекомендации по размещению СКЗИ и режиму охраны:

- помещения, в которых размещаются технические средства с установленным СКЗИ, являются режимными и должны обеспечивать конфиденциальность проводимых работ;
- размещение режимных помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств;
- размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности;
- входные двери режимных помещений должны быть оборудованы замками, обеспечивающими надежное закрытие помещений в нерабочее время;
- окна и двери должны быть оборудованы охранной сигнализацией, связанной с пультом
- централизованного наблюдения за сигнализацией;
- размещение технических средств в режимном помещении должно исключать возможность визуального просмотра конфиденциальных документов и экранов мониторов, на которых она отражается, через окна;
- в режимные помещения допускаются руководители организации Участника СЭД, сотрудники подразделения безопасности и исполнители, имеющие прямое отношение к обработке, передаче и приему конфиденциальных документов;
- системные блоки компьютеров с СКЗИ оборудуются средствами контроля вскрытия;
- ремонт и/или последующее использование системных блоков осуществляется после удаления с них программного обеспечения СКЗИ.

3. Рекомендации по обеспечению безопасности ключевой информации:

- ключевые носители и носители инсталляционных пакетов программного обеспечения СКЗИ в организации Участника СЭД берутся на поэкземплярный учет в выделенных для этих целей журналах;
- учет и хранение ключевых носителей поручается руководством организации Участника СЭД специально выделенным сотрудникам;
- для хранения ключевых носителей выделяется сейф или иное хранилище, обеспечивающее сохранность ключевой информации;
- хранение ключевых носителей и носители инсталляционных пакетов программного обеспечения СКЗИ допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение;
- рабочие и резервные криптографические ключи хранятся раздельно с обеспечением условия невозможности их одновременной компрометации;

- при транспортировке ключевых носителей создаются условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на записанную информацию;
- выведенные установленным порядком из действия ключи ЭП уничтожаются.