**Требования ФСБ (ФАПСИ) по обеспечению безопасности информации при ее защите по уровню «С» (на уровне потребителя)**

Защита информации по уровню "С" означает применение алгоритмов электронной цифровой подписи, шифрования, хеширования, реализуемыми сертифицированными органами ФСБ (ФАПСИ) средствами криптографической защиты информации (СКЗИ).

1. Требования по организационному обеспечению эксплуатации СКЗИ
	1. В организации выделяются (определяются) должностные лица, ответственные за обеспечение безопасности информации и эксплуатацию СКЗИ.
	2. В организации разрабатываются нормативные документы, регламентирующие вопросы безопасности информации и эксплуатацию СКЗИ.
	3. К работе с СКЗИ допускаются сотрудники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации СКЗИ.
2. Требования по размещению СКЗИ и режиму охраны
	1. Помещения, в которых размещаются программно-технические средства с встроенными в них СКЗИ, являются режимными и должны обеспечивать конфиденциальность проводимых работ.
	2. 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.
	3. Размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности.
	4. Входные двери режимных помещений должны быть оборудованы замками, обеспечивающими надежное закрытие помещений в нерабочее время.
	5. Окна и двери должны быть оборудованы охранной сигнализацией, связанной с пультом централизованного наблюдения за сигнализацией.
	6. Размещение технических средств в режимном помещении должно исключать возможность визуального просмотра конфиденциальных документов и экранов мониторов, на которых она отражается, через окна.
	7. В режимные помещения допускаются руководство абонента, сотрудники подразделения безопасности и исполнители, имеющие прямое отношение к обработке, передаче и приему конфиденциальных документов.
	8. Системные блоки ЭВМ с СКЗИ оборудуются средствами контроля вскрытия.
	9. Ремонт и/или последующее использование системных блоков осуществляется после удаления с них программного обеспечения СКЗИ.
3. Требования по обеспечению безопасности ключевой информации
	1. Носители секретных ключей ЭЦП, шифрования и инсталляционные дискеты с ПО СКЗИ в организации берутся на поэкземплярный учет в выделенных для этих целей журналах.
	2. Учет и хранение секретных ключей поручается руководством организации специально выделенным сотрудникам.
	3. Для хранения носителей секретных ключей ЭЦП и шифрования выделяется сейф или иное хранилище, обеспечивающее сохранность ключевой информации.
	4. Хранение ключей и инсталляционных дискет с программным обеспечением СКЗИ допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное не предусмотренное правилами пользования СКЗИ применение.
	5. Рабочие (актуальные) и резервные ключи хранятся раздельно, с обеспечением условия невозможности их одновременной компрометации.
	6. При транспортировке носителей секретной ключевой информации обеспечиваются условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на записанную ключевую информацию.

Примечание. Требования по размещению СКЗИ определяются условиями лицензирования этих средств, правилами эксплуатации сертифицированных СКЗИ и могут уточняться при подготовке автоматизированных рабочих мест уполномоченных лиц.