

Инструкция по обращению с сертифицированными ФСБ России шифровальными (криптографическими) средствами

1. Общие положения

1.1. Настоящая Инструкция регламентирует порядок обращения с сертифицированными ФСБ России шифровальными (криптографическими) средствами*, предназначенными для защиты информации, не содержащей сведений, составляющих государственную тайну, в процессе их получения, транспортировки, учета, хранения, встраивания в прикладные системы, тестирования, испытаний, передачи и установки (инсталляции), уничтожения, а также порядок допуска к работам с шифровальными (криптографическими) средствами.

Все положения настоящей Инструкции распространяются также на прикладные системы с встроенными средствами криптографической защиты информации (СКЗИ).

1.2. Основанием для использования СКЗИ является договор между клиентом (далее – Клиент) и ОАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» (далее – Банк).

1.3. Сведения об СКЗИ, включая аппаратные средства, инсталлирующие СКЗИ-носители, эксплуатационную и техническую документацию к СКЗИ, относятся к информации конфиденциального характера

1.4. К работе с СКЗИ сотрудники Клиента допускаются на основании приказов по организации после прохождения необходимой подготовки.

1.5. В организации Клиента приказом должно быть назначено лицо, уполномоченное руководить работами с шифровальными средствами. Банк вправе затребовать заверенную Клиентом копию такого приказа, а Клиент должен предоставить ее не позднее трех рабочих дней с даты получения письменного запроса.

1.6. Все сотрудники Клиента, допущенные к работе с СКЗИ, должны строго выполнять требования настоящей Инструкции в части, их касающейся.

1.7. Все сотрудники Клиента, допущенные к работе с СКЗИ, должны строго выполнять требования нормативных правовых актов Российской Федерации, относящихся к деятельности с СКЗИ, и нормативных и методических документов лицензирующего органа.

* К шифровальным (криптографическим) средствам (средствам криптографической защиты информации) согласно постановлению Правительства Российской Федерации от 29 декабря 2007 г. № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами» относятся:

а) средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

б) средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

в) средства электронной цифровой подписи – аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;

г) средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

д) средства изготовления ключевых документов (независимо от вида носителя ключевой информации);

е) ключевые документы (независимо от вида носителя ключевой информации).

1.8. Работы с СКЗИ должны проводиться с учетом нормативных документов, регламентирующих порядок разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации, а также порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

2. Требования по размещению, специальному оборудованию и охране помещений, в которых производятся работы с СКЗИ

2.1. В целях обеспечения сохранности конфиденциальных документов и технических средств СКЗИ должны размещаться в помещениях с особым режимом доступа, исключающим возможность бесконтрольного проникновения в указанные помещения посторонних лиц.

2.2. При размещении СКЗИ необходимо исключить возможность визуального доступа посторонних лиц к документам и экранам мониторов путем просмотра через окна и открытые двери.

2.3. При расположении помещения, в котором размещены СКЗИ, на первом или последнем этажах здания, а также при наличии рядом с окнами балконов, пожарных лестниц и других мест, откуда возможно проникновение в помещение посторонних лиц, окна помещения необходимо оборудовать металлическими решетками, ставнями, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению в помещение.

2.4. Технические средства, предназначенные для обработки конфиденциальной информации, должны соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности.

3. Порядок обращения с СКЗИ

3.1. Передача СКЗИ, устанавливающих СКЗИ носителей, эксплуатационной и технической документации уполномоченному представителю Клиента производится ответственным сотрудником Банка по акту. При этом ответственный сотрудник Банка заносит в журнал регистрации номер и дату составления акта приема-передачи СКЗИ, наименование организации, фамилию, имя, отчество представителя Клиента.

3.2. При транспортировке СКЗИ, устанавливающих СКЗИ носителей, эксплуатационной и технической документации должны быть обеспечены условия, исключающие возможность физических повреждений, внешнего воздействия на записанную информацию, а также ее копирования.

3.3. Все СКЗИ, устанавливающие СКЗИ носители, эксплуатационная и техническая документация к ним должны учитываться уполномоченными сотрудниками Клиента путем поэкземплярного учета в специальных журналах согласно установленной форме.

Единицей поэкземплярного учета СКЗИ является:

– для аппаратных и программно-аппаратных СКЗИ – конструктивно законченное техническое устройство;

– для программных СКЗИ – устанавливающий СКЗИ носитель (дискета, компакт-диск и т.п.).

3.4. Установка (инсталляция) СКЗИ осуществляется в соответствии с требованиями документации на СКЗИ.

3.5. Ответственными сотрудниками Клиента периодически должен проводиться контроль сохранности СКЗИ, а также всего используемого совместно с СКЗИ программного обеспечения для предотвращения внесения программно-аппаратных закладок и программ-вирусов.

3.6. При эксплуатации СКЗИ не допускается:

– снимать несанкционированные копии с ключей;

- разглашать содержимое ключевого носителя или передавать сами носители лицам, к ним не допущенным;
- выводить секретный ключ на дисплей, принтер или другие внешние устройства отображения информации;
- вставлять ключевой носитель в устройство считывания ПЭВМ в режимах, не предусмотренных штатным режимом, а также в дисководы других ПЭВМ;
- записывать на ключевой носитель постороннюю информацию;
- подключать к ПЭВМ дополнительные устройства и соединители без соответствующего предписания на возможность их совместного использования;
- работать на компьютере, если во время его начальной загрузки не проходит встроенный тест, предусмотренный в ПЭВМ;
- оставлять без контроля ПЭВМ при включенном питании и загруженном программном обеспечении СКЗИ. При кратковременном перерыве в работе рекомендуется производить гашение экрана, возобновление активности экрана производится с использованием пароля доступа;
- вносить какие-либо изменения в программное обеспечение;
- несанкционированно устанавливать, создавать и выполнять на ПЭВМ посторонние программы;
- осуществлять несанкционированное вскрытие системных блоков ПЭВМ.

4. Ответственность за нарушение требований Инструкции

За нарушение требований настоящей Инструкции виновные несут дисциплинарную либо материальную ответственность в зависимости от характера нарушения и тяжести наступивших отрицательных последствий.