Научно-производственное предприятие
“ИЖИНФОРМПРОЕКТ”

УТВЕРЖДЕНЫ

приказом от 11.01.2009 № 1

Требования

по обеспечению безопасности автоматизированного рабочего места

Редакция № 2

Ижевск 2009

1 Настоящее требования разработаны в соответствии с Федеральным Законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным Законом Российской Федерации от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи», Федеральным Законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным Законом Российской Федерации от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Постановлением Правительства Российской Федерации от 29.12.2007 № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами», Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 09.02.2005 № 66, Инструкцией 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, Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными ФСБ России от 21.02.2008 № 149/6/6-622, Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденными ФСБ России от 21.02.2008 № 149/54-144, Правилами пользования СКЗИ КриптоПро CSP ЖТЯИ.00005-02 90 07 и Инструкцией по использованию КриптоПро CSP и TLS ЖТЯИ.00015-01 90 02-05.

2 Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним,

должны обеспечивать сохранность конфиденциальной информации, СКЗИ, ключевых документов.

3 Спецпомещения выделяются с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. Окна спецпомещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

4 Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в спецпомещениях пользователей СКЗИ 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.

5 На время отсутствия пользователей СКЗИ указанное оборудование должно быть выключено или приняты организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами в их отсутствие.

6 Режим охраны спецпомещений пользователей СКЗИ, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает обладатель конфиденциальной информации. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны.

7 В спецпомещениях пользователей СКЗИ для хранения выданных им ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования,

оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ.

8 При утрате ключа от хранилища или от входной двери в спецпомещение пользователя СКЗИ 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. В обычных условиях опечатанные хранилища пользователей СКЗИ могут быть вскрыты только самими пользователями.

9 При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти спецпомещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено руководству обладателя конфиденциальной информации и (при необходимости) в ООО НПП «Ижинформпроект». При этом необходимо оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации конфиденциальной информации и к замене скомпрометированных криптоключей.

10 Средства вычислительной техники, на которых осуществляется штатное функционирование СКЗИ, рекомендуется оборудовать средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

11 Все программное обеспечение ПЭВМ, на которой будет устанавливаться СКЗИ, должно быть лицензионно чистым, при этом рекомендуется не допускать наличия средств разработки и отладки программ. Перед установкой СКЗИ необходимо проверить программное обеспечение ПЭВМ на отсутствие вирусов и программных закладок.

12 Для обеспечения защиты от НСД могут использоваться средства типа «электронный замок».

13 При осуществлении доступа в сети передачи данных следует использовать дополнительные сертифицированные средства защиты информации: межсетевые экраны, антивирусные средства.

14 Не допускается оставлять без контроля вычислительные средства, входящие в состав СКЗИ, 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.

15 При каждом включении рабочей станции с установленным СКЗИ необходимо проверять сохранность печатей системного блока и разъемов рабочей станции.

16 Пользователь должен запускать только те приложения, которые разрешены администратором безопасности. На ПЭВМ должна быть установлена только одна операционная система. Программное обеспечение, установленное на ПЭВМ, не должно иметь встроенных средств разработки и отладки программ.

17 Должны быть приняты меры по исключению вхождения пользователей в режим конфигурирования BIOS (например, с использованием парольной защиты), должна быть исключена возможность работы на ПЭВМ, если во время начальной загрузки не проходят встроенные тесты.