Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Самарский государственный экономический университет»

ИНСТРУКЦИЯ ОБ ОРГАНИЗАЦИИ И ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ХРАНЕНИЯ, ОБРАБОТКИ И ПЕРЕДАЧИ ПО КАНАЛАМ СВЯЗИ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ С ОГРАНИЧЕННЫМ ДОСТУПОМ, НЕ СОДЕРЖАЩИМ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ

Листов 12

Самара

2022 год

СОДЕРЖАНИЕ

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

ПДн	–	Персональные данные
РФ	–	Российская Федерация
СКЗИ	–	Средства криптографической защиты информации
Университет	–	Федеральное государственное автономное образовательное учреждение высшего образования «Самарский государственный экономический университет»
ФСБ России	–	Федеральная служба безопасности России

1 Общие положения

Настоящая Инструкция регулирует отношения, возникающие при реализации и эксплуатации шифровальных (криптографических) средств защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, а также регламентирует порядок обращения с шифровальными (криптографическими) средствами, а также порядок организации и обеспечения их безопасности хранения, обработки и передачи в Федеральном государственном автономном образовательном учреждении высшего образования «Самарский государственный экономический университет» (далее – Университет).

К средствам криптографической защиты информации (далее – СКЗИ) относятся:

- средства шифрования: аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче;
- средства имитозащиты: аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации;
- средства электронной подписи;
- средства кодирования: средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций;
- средства изготовления ключевых документов: аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов для шифровальных (криптографических) средств, не входящие в состав этих шифровальных (криптографических) средств;
- ключевые документы: электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с

использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах;

- аппаратные шифровальные (криптографические) средства: устройства и их компоненты, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации без использования программ для электронных вычислительных машин;
- программные шифровальные (криптографические) средства: программы для электронных вычислительных машин и их части, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации в программно-аппаратных шифровальных (криптографических) средствах, информационных системах и телекоммуникационных системах, защищенных с использованием шифровальных (криптографических) средств;
- программно-аппаратные шифровальные (криптографические) средства: устройства и их компоненты (за исключением информационных систем и телекоммуникационных систем), в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации с использованием программ для электронных вычислительных машин, предназначенных для осуществления этих преобразований информации или их части.

2 Порядок организации средств криптографической защиты информации

Данной Инструкцией необходимо руководствоваться при реализации и эксплуатации СКЗИ конфиденциального характера в следующих случаях:

- если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации (далее – РФ);
- при организации криптографической защиты информации конфиденциального характера при выполнении ими заказов на поставку товаров, выполнение работ или оказание услуг для государственных нужд согласно законодательству РФ;
- если обязательность защиты информации конфиденциального характера возлагается законодательством РФ на лиц, имеющих доступ к этой информации или наделенных полномочиями по распоряжению сведениями, содержащимися в данной информации;
- при обрабатывании информации конфиденциального характера, обладателем которой являются государственные органы или организации, выполняющие государственные заказы, в случае принятия ими мер по охране ее конфиденциальности путем использования средств криптографической защиты;
- при обрабатывании информации конфиденциального характера в государственных органах и в организациях, выполняющих государственные заказы, обладатель которой принимает меры к охране ее конфиденциальности путем установления необходимости криптографической защиты данной информации.

При организации обмена информацией конфиденциального характера Университета с государственными органами и организациями, выполняющими государственные заказы, необходимость криптографической защиты информации и выбор применяемых СКЗИ определяются данными организациями.

При организации обмена информацией, доступ к которой ограничивается по решению Университета, с организациями, не являющихся выполняющими государственные заказы, или уполномоченными ими лицами (за исключением информации, содержащей сведения, к которым в соответствии с законодательством Российской Федерации не может быть ограничен доступ), необходимость ее криптографической защиты и выбор применяемых СКЗИ определяются соглашениями между участниками обмена.

Режим защиты информации конфиденциального характера при ее обработке и хранении в Университете с использованием СКЗИ устанавливается директором Университета на основании законодательства РФ.

Используемые СКЗИ должны удовлетворять требованиям технических регламентов, оценка выполнения которых осуществляется в порядке, определяемом Федеральным законом от 27 декабря 2002 года № 184 «О техническом регулировании», а также иным требованиям по безопасности информации, устанавливаемым в соответствии с законодательством РФ.

Качество криптографической защиты информации конфиденциального характера, осуществляемой СКЗИ, обеспечивается реализацией требований по безопасности информации, предъявляемых к СКЗИ, ключевой системе СКЗИ, а также к сетям связи (системам), используемым СКЗИ с целью защиты информации при ее передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении и условиям размещения СКЗИ при их использовании.

3 Порядок эксплуатации средств криптографической защиты информации

СКЗИ эксплуатируются в соответствии с установленными в Университете правилами пользования ими. Все изменения условий использования СКЗИ, указанных в данных правилах, должны согласовываться с ФСБ России или специализированной организацией, проводившей тематические исследования СКЗИ.

СКЗИ, находящиеся в эксплуатации, должны подвергаться контрольным тематическим исследованиям, конкретные сроки проведения которых определяются Университетм по согласованию с разработчиком СКЗИ, специализированной организацией и ФСБ России.

СКЗИ подлежат поэкземплярному учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов (условных наименований) и регистрационных номеров поэкземплярного учета СКЗИ определяет ФСБ России.

Организация поэкземплярного учета используемых СКЗИ возлагается на сотрудника Университета, ответственного за обеспечение безопасности персональных данных (далее – ПДн).

Контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, а также условий производства ключевых документов, осуществляется в соответствии с требованиями Федерального закона от 26 декабря 2008 года № 294 «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля».

Контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, осуществляется:

- Университетм;
- ФСБ России в рамках контроля за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи.

С целью оценки обоснованности и достаточности мер, принятых для защиты информации конфиденциального характера, Университет вправе обратиться в ФСБ России с просьбой о проведении контроля за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования СКЗИ.

4 Порядок обращения со средствами криптографической защиты информации

Сотрудники Университета допускаются к работе с шифровальными (криптографическими) средствами на основании приказа директора Университета после прохождения необходимой подготовки. В подготовку может входить как проверка знания действующего законодательства РФ в области обработки и защиты ПДн, так и знание устройства самих СКЗИ.

Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету в специальном «Журнале поэкземплярного учета средств криптографической защиты информации», утвержденном приказом директора Университета. Единицей поэкземплярного учета программных СКЗИ является инсталляционная дискета или компактный диск (CD-ROM), для аппаратных средств – единица оборудования. Передаваемые (распространяемые) шифровальные (криптографические) средства должны иметь учетные номера. Все шифровальные (криптографические) средства реализуются (распространяются) вместе с правилами пользования ими.

При транспортировке СКЗИ должны обеспечиваться условия, исключающие возможность неконтролируемого доступа к ним, их физического повреждения и внешнего воздействия. Категорически запрещается нарушать оригинальную упаковку шифровальных (криптографических) средств. Осуществляют транспортировку шифровальных (криптографических) средств сотрудники Университета, допущенные согласно приказу директора Университета.

Передачу шифровальных (криптографических) средств сторонней организации производит ответственный сотрудник Университета с оформлением соответствующего акта. Данный сотрудник регистрирует номер и дату акта приема-передачи шифровальных (криптографических) средств, наименования организации, фамилию, имя, отчество представителя в «Журнале поэкземплярного учета средств криптографической защиты информации».

Сотрудником Университета, ответственными за обеспечение безопасности ПДн, с установленной периодичностью должен проводиться контроль сохранности СКЗИ в Университете, а также контроль за соблюдением условий их использования.

5 Требования к помещениям, в которых производятся работы со средствами криптографической защиты информации

Специальное оборудование, охрана и режим в помещениях, в которых осуществляется хранение шифровальных (криптографических) средств (далее – помещения), обеспечивают безопасность СКЗИ и ограничение неконтролируемого доступа к ним.

Пользователи СКЗИ хранят инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение. Пользователи СКЗИ предусматривают также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптоключей.

Доступ лиц в защищаемые помещения должен быть ограничен в соответствии со служебной необходимостью и определяться приказом директора Университета.

Помещения должны быть оборудованы прочными входными дверями, препятствующими свободному доступу, имеющими средства контроля вскрытия. Дубликаты ключей от входных дверей должны храниться в сейфе лица, ответственного за обеспечение безопасности ПДн. Окна помещений должны быть оборудованы средствами, препятствующими неконтролируемому проникновению в помещения. На дверях и оконных стеклах должны быть установлены датчики охранной сигнализации. В помещении должна быть установлена система пожарной сигнализации.

По окончании рабочего дня ответственный сотрудник Университета обязан закрыть помещение, опечатать помещение личной номерной печатью, сдать помещение под охрану. При вскрытии помещений необходимо проверять целостность печатей и замков. В случае нарушения целостности печатей или замков данный сотрудник обязан немедленно сообщить об этом директору Университета.

6 Ответственность за нарушение требований инструкции

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

В случае если не исполнение или ненадлежащее исполнение сотрудниками Университета своих обязанностей, предусмотренных настоящей Инструкцией повлекли за собой значительные финансовые потери Университета, то они могут быть привлечены к ответственности в соответствии с действующим законодательством РФ.

7 ЛИСТ ОЗНАКОМЛЕНИЯ

ФИО	**Должность**	**Подпись,Дата**