Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Самарский государственный экономический университет»

ПОРЯДОК РАЗРЕШИТЕЛЬНОГО ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К АВТОМАТИЗИРОВАННЫМ РАБОЧИМ МЕСТАМ СО СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Листов 9

Самара

2022 год

СОДЕРЖАНИЕ

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

АРМ	–	Автоматизированное рабочее место
ИСПДн ДА	–	Информационная система персональных данных документов об образовании и государственной итоговой аттестации
НСД	–	Несанкционированный доступ
ОС	–	Операционная система
ПДн	–	Персональные данные
ПО	–	Программное обеспечение
РФ	–	Российская Федерация
СКЗИ	–	Средство криптографической защиты информации
Университет	–	Федеральное государственное автономное образовательное учреждение высшего образования «Самарский государственный экономический университет»
ФСБ России	–	Федеральная служба безопасности России

1 Общие положения

Настоящий Порядок описывает порядок разрешительного доступа эксплуатирующего персонала, пользователей и администраторов информационной системы персональных данных документов об образовании и государственной итоговой аттестации Федерального государственного автономного образовательного учреждения высшего образования «Самарский государственный экономический университет» (далее – ИСПДн ДА ФГАОУ ВО «СГЭУ») к автоматизированным рабочим местам (далее – АРМ) с установленными средствами криптографической защиты информации (далее – СКЗИ).

2 Требования к размещению и оснащению технических средств с установленными СКЗИ

При размещении технических средств ИСПДн ДА ФГАОУ ВО «СГЭУ» с установленными СКЗИ необходимо принимать следующие меры:

- исключение несанкционированного доступа в помещения, в которых размещены технические средства с установленными СКЗИ, посторонних лиц, не являющихся сотрудниками Университета, допущенными к работе в данных помещениях;
- обеспечение контроля за действиями указанных лиц и обеспечение невозможности негативных действий с их стороны на технические средства, на которых эксплуатируется СКЗИ, включая СКЗИ и защищаемую информацию;
- обеспечение сотрудниками Университета сохранности доверенных им конфиденциальных сведений, включая ключевую информацию посредством специальной внутренней планировки и расположения АРМ в помещениях.

Оснащение технических средств с установленными СКЗИ необходимо производить в соответствии с нижеприведенными требованиями.

На технических средствах с установленными СКЗИ должно использоваться только лицензионное программное обеспечение (далее – ПО), либо ПО, сертифицированное ФСБ России. Указанное ПО не должно содержать средств разработки или отладки приложений, а также возможностей, позволяющих оказывать воздействие на функционирование СКЗИ. В случае технологических потребностей Университета в использовании иного ПО, его применение должно быть санкционировано сотрудником, ответственным за обеспечение безопасности персональных данных (далее – ПДн) в Университете.

Установленное на технические средства ПО не должно содержать в себе возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;
- модифицировать собственный код и код других подпрограмм;
- модифицировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;
- несанкционированное модифицировать файлы, содержащие исполняемые кода при их хранении на жестком диске;
- использовать недокументированные фирмами-разработчиками функции.

Программные модули СКЗИ (прикладного ПО со встроенным СКЗИ) должны быть доступны только по чтению/запуску, в атрибутах файлов следует запретить запись и модификацию.

На каждом АРМ, оснащенном СКЗИ, одновременно может быть установлена только одна разрешенная операционная система (далее – ОС), средствами BIOS которой необходимо обеспечить следующее:

- определение установок, исключающих возможность загрузки ОС, отличной от установленной на жестком диске: отключение возможности загрузки с гибкого диска, привода CD-ROM и прочие нестандартные виды загрузок ОС, включая сетевую;
- запрет возможности отключения пользователями PCI устройств при использовании программно-аппаратного комплекса защиты от несанкционированного доступа (далее – НСД), устанавливаемого в PCI-E-разъем АРМ;
- защита входа в BIOS паролем, который должен быть известен только администратору ПС ГИС СО «МФЦ» и быть отличным от пароля входа в ОС;
- исключение возможности работы на АРМ, если во время начальной загрузки не проходят встроенные тесты;

Сотруднику, ответственному за обеспечение безопасности ПДн в Университете, необходимо провести опечатывание системного блока АРМ с установленным СКЗИ, исключающее возможность несанкционированного изменения аппаратной части АРМ.

3 Защита информации от несанкционированного доступа

В рамках подсистемы криптографической защиты информации в ИСПДн ДА ФГАОУ ВО «СГЭУ» при использовании СКЗИ необходимо принимать следующие организационные меры:

- предоставить права доступа к АРМ с установленным СКЗИ только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на СКЗИ;
- запретить осуществление несанкционированного копирования ключевых носителей;
- запретить передачу ключевых носителей лицам, к ним не допущенным;
- запретить использование ключевых носителей в режимах, не предусмотренных правилами пользования СКЗИ;
- запретить запись на ключевые носители посторонней информации;
- запретить оставлять без контроля технические средства, на которых эксплуатируется СКЗИ после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки;
- хранить ключевые в запираемых и опечатываемых сейфах. Пользователь несет персональную ответственность за хранение личных ключевых носителей;
- сдать ключевые носители в соответствии с порядком, установленным при увольнении или отстранении от исполнения обязанностей;
- немедленно уведомлять сотрудника, ответственного за обеспечение безопасности ПДн, о фактах утраты или недостачи ключевых носителей, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению конфиденциальной информации;
- запрещается разглашать содержимое носителей ключевой информации и передавать носители лицам к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п., иные средства отображения информации;
- перед началом процесса установки ПО со встроенными модулями СКЗИ, либо автономных программных модулей СКЗИ должен осуществляться контроль целостности устанавливаемого ПО;
- при каждом запуске АРМ с установленным СКЗИ должен осуществляться контроль целостности программного обеспечения, входящего в состав СКЗИ, самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ;

- сотрудник, ответственный за обеспечение безопасности ПДн, должен периодически (не реже 1 раза в год) менять пароль на вход в BIOS;
- в случае обнаружения «посторонних» (незарегистрированных) программ или нарушения целостности программного обеспечения работа должна быть прекращена;
- пользователь должен запускать только те приложения, которые разрешены администратором ИСПДн ДА ФГАОУ ВО «СГЭУ»;
- сотрудник, ответственный за обеспечение безопасности ПДн, должен сконфигурировать ОС, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль выполненных настроек в соответствии со следующими требованиями:
  - не использовать нестандартные, измененные или отладочные ОС;
  - исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой;
  - исключить возможность удаленного управления, администрирования и модификации ОС и ее настроек;
  - правом установки и настройки ОС и СКЗИ должен обладать только сотрудник, ответственный за обеспечение безопасности ПДн;
  - ОС должна быть настроена только для работы с СКЗИ. Все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);
  - всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права;
  - кроме того, необходимо организовать затирание (по окончании сеанса работы СКЗИ) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ. Если это не выполнимо, то ОС должна использоваться в однопользовательском режиме и на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.
  - должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии;
  - необходимо регулярно устанавливать пакеты обновления безопасности ОС, обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС;
  - в случае подключения АРМ с установленным СКЗИ к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения

файлов и скриптовых объектов (JavaScript, VBScript, ActiveX), полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети;

- при использовании СКЗИ на АРМ, подключенных к общедоступным сетям связи, с целью исключения возможности НСД к системным ресурсам используемых ОС, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты;
- исключить одновременную работу в ОС с работающим СКЗИ и загружаемой ключевой информацией нескольких пользователей;
- организовать и использовать систему аудита, организовать регулярный анализ результатов аудита;
- организовать и использовать комплекс антивирусной защиты.