федеральное государственное бюджетное образовательное учреждение высшего образования
«ОМСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»
Министерства здравоохранения Российской Федерации

УТВЕРЖДАЮ
Ректор ФГБОУ ВО ОмГМУ
Минздрава России
_____ М.А. Ливзан
«19» 09 2024 г.

ИНСТРУКЦИЯ

ПО ПОРЯДКУ ОБРАЩЕНИЯ СО СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

КОНТРОЛЬНЫЙ

Омск 2024

ПРЕДИСЛОВИЕ

1. РАЗРАБОТАНА заведующим сектора информационной безопасности Ключенко А.А.

2. ПРИНЯТА ученым советом 19.09.2024 г., протокол № 10.

3. ВВЕДЕНА в действие с 23.09.2024 г. распоряжением от 20.09.2024 г. впервые.

СОДЕРЖАНИЕ

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящая Инструкция по порядку обращения со средствами защиты информации в информационных системах персональных данных ФГБОУ ВО ОмГМУ Минздрава России (далее, соответственно – ИС, Инструкция) регламентирует порядок обращения со средствами защиты информации в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты информации, обрабатываемой с использованием средств автоматизации.

1.2 Требования настоящей Инструкции обязательны для сотрудников ФГБОУ ВО ОмГМУ Минздрава России, обрабатывающих информацию в информационных системах персональных данных.

2 НОРМАТИВНЫЕ ССЫЛКИ

В настоящей Инструкции использованы ссылки на следующие документы:

– Федеральный закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закона от 27 июля 2006 № 152-ФЗ «О персональных данных».

3 ОБЩИЕ ПОЛОЖЕНИЯ

3.1 В настоящей Инструкции используются следующие понятия и определения:

- Доступ к информации – возможность получения информации и ее использования.

- Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

- Контролируемая зона – пространство (территория, здание, часть здания), в

котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

- Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации, не являющееся криптосредством.

3.1 Для обеспечения безопасности информации при ее обработке в ИС должны использоваться сертифицированные в системе сертификации ФСТЭК России СЗИ (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации).

4 УЧЕТ СЗИ

4.1 Инсталлирующие СЗИ носители и установленные СЗИ подлежат поэкземплярному учету администратором информационной безопасности (далее – ИБ).

4.2 Программные СЗИ учитываются совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные СЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СЗИ учитываются также совместно с соответствующими аппаратными средствами.

4.3 Эксплуатационная и техническая документация к СЗИ подлежит поэкземплярному учету администратором ИБ.

4.4 СЗИ, а также эксплуатационная и техническая документация к СЗИ должны быть упакованы в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия.

4.5 Полученные упаковки с СЗИ, а также с эксплуатационной и технической документацией к ним, вскрываются администратором ИБ. Администратор ИБ проверяет целостность упаковки и содержимого.

4.6 Уничтожение СЗИ:

4.6.1 СЗИ уничтожаются (утилизируются) по решению комиссии по проведению мероприятий по защите информации совместно с Администратором ИБ.

4.6.2 Намеченные к уничтожению (утилизации) СЗИ изымаются из аппаратных средств, с которыми они функционировали. При этом СЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СЗИ процедура удаления программного обеспечения СЗИ, и они полностью отсоединены от аппаратных средств.

4.6.3 Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения используются после уничтожения СЗИ без ограничений.

4.7 Эксплуатационная и техническая документация к СЗИ уничтожается путем сжигания или с помощью любых бумагорезательных машин.

5 КОНТРОЛЬ БЕЗОПАСНОСТИ СЗИ

5.1 Текущий контроль за организацией и обеспечением функционирования СЗИ возлагается на Ответственного за обработку и защиту информации и Администратора ИБ в пределах их полномочий.

6 МОДИФИКАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И АППАРАТНЫХ И ТЕХНИЧЕСКИХ СРЕДСТВ

6.1 Все изменения конфигурации ИС должны производиться только на основании заявок пользователей ИС, согласованных с Ответственным за

обработку и защиту информации, на имя Администратора ИБ.

6.2 Право внесения изменений в конфигурацию ИС предоставляется:

- в отношении системных и прикладных программных средств, а также в отношении аппаратных средств – уполномоченному Администратору ИС;
- в отношении СЗИ – уполномоченному Администратору ИБ.

6.3 Изменение конфигурации ИС, кроме уполномоченных работников, запрещено.

6.4 Установка, изменение (обновление) и удаление системных и прикладных программных средств производится Администратором ИС.

6.5 Подготовка модификаций программного обеспечения (далее – ПО) средств вычислительной техники (далее – СВТ), тестирование, стендовые испытания и передача исходных текстов, документации и дистрибутивных носителей программ в архив эталонных дистрибутивов, и другие необходимые действия производятся Администратором ИС.

6.6 Установка и обновление общего программного обеспечения на СВТ производится с оригинальных лицензионных дистрибутивных носителей (компакт дисков и т.п.), полученных установленным порядком, а прикладного ПО – с эталонных копий программных средств.

6.7 Все добавляемые программные и аппаратные компоненты должны быть предварительно установленным порядком проверены на работоспособность, а также отсутствие опасных функций.

6.8 После установки (обновления) ПО Администратор ИС должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с ее (его) формуляром. Администратор ИБ должен проверить работоспособность ПО и правильность настройки СЗИ.

6.9 При изъятии СВТ из состава ИС его передача на склад, в ремонт или в

другое подразделение для решения иных задач осуществляется только после того, как Администратор ИБ снимет с данной СВТ средства защиты и предпримет необходимые меры для затирания защищаемой информации, которая хранилась на дисках СВТ. Факт уничтожения защищаемой информации, находившейся на диске СВТ, оформляется актом за подписью Администратора ИБ.

7 ЭКСТРЕННАЯ МОДИФИКАЦИЯ (ОБСТОЯТЕЛЬСТВА ФОРС-МАЖОР)

7.1 В исключительных случаях (сбой ПО, не позволяющий продолжить работу), требующих безотлагательного изменения ПО, допускается корректировка программ непосредственно на СВТ. Факт внесения изменений в ПО СВТ фиксируется актом за подписями Администратора ИС, Администратора ИБ и пользователя данного СВТ. В акте указывается причина модификации, перечисляются файлы, подвергшиеся изменению, и указывается лицо(а), проводившее изменения.

7.2 В течение следующего дня после составления акта Администратором ИС, Администратором ИБ при участии пользователей ИС выясняются причины и состав проведенных экстренных изменений, и принимается решение о необходимости подготовки исправительной модификации ПО или восстановления ПО СВТ с эталонной копии. Необходимость участия в разбирательстве пользователя ИС определяется руководством. Результат разбирательства оформляется в виде согласованного решения и хранится у Администратора ИС, копии передаются Администратору ИБ.

8 ОТВЕТСТВЕННОСТЬ

8.1 Пользователи ИС несут персональную ответственность за сохранность полученных СЗИ, эксплуатационной и технической документации к СЗИ, за соблюдение положений настоящей Инструкции.

8.2 Ответственный за обработку и защиту информации в ИС несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности обработки информации с использованием СЗИ лицензионным требованиям и условиям эксплуатационной и технической документации к СЗИ, а также настоящей Инструкции.

ЛИСТ СОГЛАСОВАНИЯ

СОГЛАСОВАНО
Проректор по последипломному образованию

_____ А.С. Колчин

«12» 09 2024 г.

СОГЛАСОВАНО
Начальник ОА и ИТ

_____ Р.А. Ахмеров

«09» 09 2024 г.

СОГЛАСОВАНО
Начальник юридического отдела

_____ О.В. Глевская

«09» 09 2024 г.

СОГЛАСОВАНО
Заместитель начальника управления организации и контроля качества образования

_____ С.В. Плоткина

«12» 09 2024 г.