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 АНТИВИРУСНОЙ ЗАЩИТЕ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ

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 определяет требования к организации антивирусной защиты автоматизированных рабочих мест (далее – АРМ) в ФГБОУ ВО ОмГМУ Минздрава России не входящих в состав информационных систем персональных данных от разрушающего воздействия компьютерных вирусов и устанавливает ответственность работников эксплуатирующих АРМ.

1.2 Действие настоящей Инструкции распространяется на пользователей (далее - Пользователи) и администратора (далее - Администратор) автоматизированных рабочих мест (далее - АРМ) ФГБОУ ВО ОмГМУ Минздрава России.

1.3 Настоящая Инструкция является локальным нормативным актом Университета, выполнение требований которого обязательно для всех структурных подразделений Университета, должностных лиц и сотрудников, участвующих в работе с АРМ.

2 НОРМАТИВНЫЕ ССЫЛКИ

2.1 Настоящая Инструкция разработана с учетом следующих положений, законодательных и нормативно-правовых актов:

– П-289 «Об информационной безопасности ОмГМУ».

3 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И ОБОЗНАЧЕНИЯ

3.1 В настоящей Инструкции применяются следующие обозначения и сокращения:

ФСТЭК – Федеральная служба по техническому и экспортному контролю;

ПО – программное обеспечение;

ИС – информационная система;

АРМ – автоматизированное рабочее место.

4 ОБЩИЕ ПОЛОЖЕНИЯ

4.1 Под антивирусными средствами в данной инструкции понимаются специализированные программные средства защиты информации, предназначенные для обнаружения фактов вирусного воздействия на компоненты АРМ.

4.2 Администрирование и обновление автономных клиентов антивирусной защиты происходит следующим образом: все операции по настройке, администрированию и обновлению производятся сотрудниками отдела автоматизации и информационных технологий (далее – Администратор).

4.3 Средство антивирусной защиты должно быть сертифицировано регуляторами (ФСТЭК, ФСБ).

4.4 Обновление антивирусных баз должно производиться ежедневно.

4.5 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая от сторонних лиц и организаций.

4.6 Ответственность за выполнение положений данной Инструкции возлагается на пользователей АРМ и сотрудников отдела автоматизации и информатизации.

5 ОБЩИЕ ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ АРМ

5.1 Пользователю запрещено изменять настройки антивирусного программного обеспечения или отключать его.

5.2 Пользователь должен оповещать Администратора о локальных сообщениях антивирусного программного обеспечения на его АРМ.

5.3 Устанавливаемое системное и прикладное программное обеспечение (ПО) на средствах вычислительной техники должно быть проверено на отсутствие компьютерных вирусов. Непосредственно после установки (изменения) ПО

должна быть выполнена антивирусная проверка на АРМ лицом, установившим (изменившим) ПО.

5.4 При работе с машинными носителями информации, полученными из сторонних организаций, пользователь обязан перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.

5.5 Пользователи АРМ обязаны проводить периодическое тестирование установленного на АРМ всего ПО на предмет отсутствия компьютерных вирусов в течение рабочего дня, а также периодическое (не реже 1 раза в неделю) полное тестирование АРМ на вирусы.

5.6 Пользователь должен оповещать Администратора о любых аномалиях в работе АРМ. К таким аномалиям могут относиться:

- На компьютере появляются неожиданные сообщения, изображения или звуковые сигналы.
- Программы без вашего участия могут запускаться или подключаться к интернету.
- В вашем почтовом ящике много сообщений без адреса отправителя и темы письма.
- Компьютер работает медленно или часто зависает.
- При включении компьютера операционная система не загружается.
- Файлы и папки могут исчезнуть, или их содержимое может измениться.
- Всплывает множество системных сообщений об ошибке.
- Браузер зависает или ведет себя неожиданным образом. Например, вы не можете закрыть вкладку.

5.7 В случае обнаружения компьютерного вируса пользователи обязаны:

- приостановить работу на АРМ.
- немедленно поставить в известность о факте обнаружения файлов, зараженных вирусом, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе.

– совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.

– провести «лечение» зараженных вирусом файлов штатными антивирусными средствами.

– при невозможности «лечения» уничтожить зараженные вирусом файлы способом, исключающим их восстановление.

6 ОБЩИЕ ОБЯЗАННОСТИ АДМИНИСТРАТОРА

6.1 Администратор участвует в развертывании и управлением системой антивирусной защиты в ИС.

6.2 Ответственность за организацию и установление порядка проведения антивирусной защиты АРМ возлагается Администратора.

6.3 Контроль обновлений антивирусных средств и антивирусных баз.

6.4 Обеспечение функционирования и поддержания работоспособности системы антивирусной защиты

ЛИСТ СОГЛАСОВАНИЯ

СОГЛАСОВАНО
Проректор по последипломному образованию
_____ А.С. Колчин
«12» 09 2024 г.

СОГЛАСОВАНО
Начальник юридического отдела
_____ О.В. Глевская
«09» 09 2024 г.

СОГЛАСОВАНО
Начальник ОА и ИТ
_____ Р.А. Ахмеров
«09» 09 2024 г.

СОГЛАСОВАНО
Заместитель начальника управления организации и контроля качества образования
_____ С.В. Плоткина
«11» 09 2024 г.