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.

ПОЛОЖЕНИЕ

О РЕГЛАМЕНТЕ АНТИВИРУСНОЙ ЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

КОНТРОЛЬНЫЙ

Омск 2024

ПРЕДИСЛОВИЕ

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

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

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

СОДЕРЖАНИЕ

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящее Положение предназначено для всех работников ФГБОУ ВО ОмГМУ Минздрава России, имеющих доступ к информационным системам персональных данных ФГБОУ ВО ОмГМУ Минздрава России (далее – Организация, ИС).

1.2 Положение устанавливает требования и ответственность при организации защиты информации от воздействия вредоносных компьютерных вирусов.

1.3 Положение регулирует вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля при работе в ИС.

2 НОРМАТИВНЫЕ ССЫЛКИ

2.1 Настоящее положение разработано с учетом следующих положений, законодательных и нормативно-правовых актов:

– П-289 «Об информационной безопасности ФГБОУ ВО ОмГМУ Минздрава России».

3 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И ОБОЗНАЧЕНИЯ

3.1 В настоящем положении применяются следующие обозначения и сокращения:

ФСТЭК – Федеральная служба по техническому и экспортному контролю;

ПО – программное обеспечение;

ИС – информационная система;

АРМ – автоматизированное рабочее место.

4 ОБЕСПЕЧЕНИЕ АНТИВИРУСНОЙ ЗАЩИТЫ

4.1 Порядок организации антивирусной защиты.

4.2 Для организации антивирусной защиты ИС допускаются к использованию только сертифицированные Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК России) лицензионные антивирусные средства общего применения.

4.3 Антивирусное средство защиты должно быть установлено на все средства вычислительной техники (далее - СВТ) (при наличии технической возможности), входящие в ИС.

4.4 В ИС права по управлению (администрированию) средствами антивирусной защиты предоставлены только сотрудникам отдела автоматизации и информационных технологий.

4.5 Разработка и осуществление мероприятий по проведению антивирусного контроля осуществляется ответственным за обработку и защиту информации с привлечением (при необходимости) администратора информационной безопасности и /или специалистов организации, имеющей лицензию ФСТЭК России на соответствующие виды деятельности.

4.6 Должностные лица не должны допускать использования в ИС программного обеспечения и данных, не связанных с выполнением должностных обязанностей.

4.7 Расширенный антивирусный контроль проводится администратором информационной безопасности не реже одного раза в месяц и при необходимости, в случае подозрений в заражении вирусной программой.

4.8 При загрузке, открытии или исполнении объектов (файлов) из внешних источников средствами антивирусной защиты проводится автоматическая проверка объектов (файлов).

4.9 Порядок проведения антивирусного контроля.

4.10 Устанавливаемое (изменяемое) программное обеспечение предварительно проверяется администратором информационной безопасности на отсутствие вирусов. Непосредственно после установки (изменения)

программного обеспечения компьютера, должна быть выполнена антивирусная проверка администратором информационной безопасности.

4.11 При загрузке компьютера средствами антивирусной защиты проводится антивирусный контроль в автоматическом режиме.

4.12 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь ИС самостоятельно или вместе с администратором информационной безопасности проводит внеочередной антивирусный контроль своей рабочей станции для определения факта наличия или отсутствия компьютерного вируса.

4.13 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи ИС обязаны:

– приостановить работу;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя ФГБОУ ВО ОмГМУ Минздрава России и администратора информационной безопасности, 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 или уничтожение зараженных файлов.

4.14 Администратор информационной безопасности обеспечивает получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

4.15 Контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов) обеспечивается путем автоматического получения или предварительного скачивания обновлений из официальных

источников, например, с сервера обновлений производителя антивирусного средства.

4.16 Применяемые в ИС системы обнаружения вторжений должны включать компоненты регистрации событий безопасности (датчики), компоненты анализа событий безопасности и распознавания компьютерных атак (анализаторы) и базу решающих правил, содержащую информацию о характерных признаках компьютерных атак.

4.17 Обнаружение (предотвращение) вторжений должно осуществляться на внешней границе ИС (системы обнаружения вторжений уровня сети) и (или) на внутренних узлах (системы обнаружения вторжений уровня узла), определяемых администратором ИБ.

4.18 Права по управлению (администрированию) системами обнаружения вторжений предоставляются только сотрудникам отдела автоматизации и информационных технологий.

4.19 В ИС обеспечивается централизованное управление (администрирование) компонентами системы обнаружения вторжении.

4.20 Обновление базы решающих правил системы обнаружения вторжений предусматривает:

– получение уведомлений о необходимости обновлений и непосредственном обновлении базы решающих правил;

– получение из доверенных источников и установку обновлений базы решающих правил;

– контроль целостности обновлений базы решающих правил.

5 ОТВЕТСТВЕННОСТЬ ПРИ ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ

5.1 Ответственность за организацию антивирусной защиты ИС в соответствии с требованиями настоящего Регламента возлагается на администратора информационной безопасности.

5.2 Ответственность за соблюдение требований настоящего Регламента возлагается на администратора информационной безопасности, администратора ИС и пользователей, эксплуатирующих ИС.

ЛИСТ СОГЛАСОВАНИЯ

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

СОГЛАСОВАНО
Начальник юридического отдела
_____ О.В. Глевская
«11» 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
«12» 09 2024 г.