Федеральное государственное бюджетное профессиональное образовательное учреждение «Электростальский медицинский колледж Федерального медико-биологического агентства»

**УТВЕРЖДАЮ**
Директор ФГБПОУ
ЭМК ФМБА России
_____Н.Н. Шарапина


# ПОЛОЖЕНИЕ О ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Рассмотрено и рекомендовано
к утверждению на заседании
педагогического совета
Протокол № 4 « 12 » января 2021 г.

г. Электросталь, 2021 г.

# Организация антивирусной защиты информационных систем персональных данных

## I. Общие положения

1. Настоящее положение определяет организацию защиты информации в информационных системах персональных данных Колледжа (далее – ИСПДн), от воздействия компьютерных вирусов, а также устанавливает ответственность за состояние антивирусной защиты.

## II. Организация антивирусной защиты

2. В ИСПДн используются сертифицированные по требованиям безопасности информации ФСТЭК и (или) ФСБ России средства антивирусной защиты. Установка средств антивирусной защиты и настройка параметров антивирусного контроля осуществляется в соответствии с руководствами, находящимися на установочных дисках средств антивирусной защиты.

3. Ответственность за своевременную установку и переустановку антивирусного средства, поддержание его в рабочем состоянии, контроль за своевременным обновлением антивирусных баз возлагается на администратора информационной безопасности (далее – Администратор ИБ).

## III. Применение средств антивирусной защиты

4. Установку и настройку средства антивирусной защиты осуществляет Администратор ИБ или организация, имеющая лицензию на деятельность по технической защите конфиденциальной информации (далее – Лицензиат). Пользователю автоматизированного рабочего места (далее – АРМ) запрещается самостоятельно изменять настройки средств антивирусной защиты.

5. Проверка файлов, размещенных на жестких дисках АРМ пользователей и серверов, а также подключаемых съемных машинных носителей осуществляется в автоматическом режиме.

6. Антивирусному контролю подлежат все файлы без исключения (текстовые, графические, исполняемые, архивные, служебные, системные и т.д.).

7. Разархивирование и обработка входящей информации проводится после ее проверки на наличие компьютерных вирусов непосредственно на носителе, содержащем эту информацию.

## IV. Действия при обнаружении вирусов

8. При возникновении подозрения на наличие компьютерного вируса, пользователь совместно с Администратором ИБ или администратором ИСПДн проводит внеочередной антивирусный контроль носителей информации.

9. В случае обнаружения средством антивирусной защиты зараженного компьютерным вирусом файла:

а) пользователь:

– приостанавливает работу;

– немедленно ставит в известность о факте обнаружения вируса Администратора ИБ или Лицензиата;

б) Администратор ИБ или администратор ИСПДн:

– оповещает других пользователей, ранее работавших с данным файлом;

– проводит лечение или уничтожение (при невозможности лечения) зараженного файла;

– принимает решение о лечении (уничтожении) системных и служебных файлов.

## V. Обновление базы данных вредоносных компьютерных программ (вирусов)

10. Обновление базы данных вредоносных компьютерных программ (вирусов) предусматривает:

1) получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных вредоносных компьютерных программ (вирусов);

2) получение из доверенных источников и установку обновлений базы данных вредоносных компьютерных программ (вирусов);

3) контроль целостности обновлений базы данных вредоносных компьютерных программ (вирусов).

11. При наличии технической возможности в ИСПДн обеспечивается централизованное управление обновлением базы данных вредоносных компьютерных программ (вирусов).

12. Обновление баз данных вредоносных компьютерных программ (вирусов) проводится каждый день в автоматическом режиме в случае подключения АРМ и серверов к локально-вычислительной сети Колледжа в информационно-коммуникационной сети «Интернет», для автономных АРМ – Администратором ИБ, Администратором ИСПДн или Лицензиатом с баз данных вредоносных компьютерных программ (вирусов), записанных на внешний машинные носитель информации, не реже 1 раза в неделю.

13. Для обновления средств антивирусной защиты, установленных на автономных АРМ, Администратор ИБ или администратор ИСПДн использует сертифицированное программное обеспечение для загрузки обновлений средства

антивирусной защиты.

## VI. Ответственность за состояние антивирусной защиты

14. Ответственность за организацию антивирусной защиты ИСПДн возлагается на администратора ИБ.

15. Ответственность за проведение мероприятий антивирусного контроля на конкретном АРМ и соблюдение положений организации антивирусной защиты возлагается на администратора ИБ и пользователя ИСПДн в рамках обязанностей, определенных настоящим положением.

16. Периодический контроль за состоянием антивирусной защиты ИСПДн, а также за соблюдением антивирусного контроля осуществляется ответственным за обеспечение безопасности персональных данных в ИСПДн (Администратором ИБ или Лицензиатом).