Приложение №6
к приказу УФИЦ РАН
от «___» _____20___г.
№ _____

ПОЛИТИКА
антивирусной защиты

1 Общие положения

1.1 Настоящая Политика определяет требования к УФИЦ РАН защиты информационной инфраструктуры УФИЦ РАН от воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее - вредоносного ПО), устанавливает ответственность руководителей и сотрудников за их выполнение.

1.2 Целью мероприятий является обеспечение антивирусной защиты информационной инфраструктуры, включающая обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

1.3 Задачами антивирусной защиты являются:

1.3.1 проведение профилактических работ с применением антивирусных диагностических средств;

1.3.2 непрерывное обеспечение защиты информации от действия вредоносных программ.

1.4 Компоненты информационной инфраструктуры, подлежащие защите от вирусов:

1.4.1 интернет-шлюзы, установленные в точках подключения к сетям общего пользования, а также ведомственным сетям;

1.4.2 сервера;

1.4.3 аппаратные средства информационной инфраструктуры;

1.4.4 средства вычислительной техники.

1.5 Основные источники вирусов:

1.5.1 съемный носитель (дискета, флеш-карта, CD-ROM, DVD-ROM, мобильное дисковое устройство) на котором находятся зараженные вирусом файлы;

1.5.2 локальная сеть и внешняя информационно-телекоммуникационная сеть;

1.5.3 жесткий диск, на который попал вирус в результате работы с зараженными программами.

2 Реализация антивирусной защиты

2.1 В УФИЦ РАН обеспечивается антивирусная защита информационной инфраструктуры средством Kaspersky Endpoint Security, включающая обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования

компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

2.2 Реализация антивирусной защиты предусматривает:

2.2.1 централизованную установку, конфигурирование и управление средствами антивирусной защиты;

2.2.2 предоставление доступа средствам антивирусной защиты к информационной инфраструктуре;

2.2.3 проведение периодических проверок информационной инфраструктуры, с целью сканирования на наличие вирусов, в автоматическом режиме;

2.2.4 проверку в режиме реального времени объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов. Обязательному входному антивирусному контролю подлежит любая информация, поступающая на средства вычислительной техники, входящие в состав АРМ. программные средства общего и специального назначения, любая информация (текстовые файлы любых форматов, файлы: данных, исполняемые файлы), получаемая и передаваемая по каналам передачи данных, а также информация на съемных машинных носителях информации (CD-ROM, Flash-накопителях и т.п.). Контроль исходящей информаций необходимо проводить непосредственно перед ее отправкой (записью на съемный машинный носитель информации);

2.2.5 оповещение ответственного за управление (администрирование) подсистемой безопасности при обнаружении вредоносных компьютерных программ (вирусов);

2.2.6 определение и выполнение действий по реагированию на обнаружение в ЗОКИИ, подвергшихся заражению вредоносными компьютерными программами (вирусами).

2.3 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 самостоятельно или совместно с ответственным за управление (администрирование) подсистемой безопасности должен провести внеочередной антивирусный контроль своей рабочей станции.

3 Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

3.1 Для средства антивирусной защиты Kaspersky Endpoint Security обеспечено обновление базы данных признаков вредоносных компьютерных программ (вирусов).

3.2 Обновление базы антивирусной проводится ежедневно.

3.3 Обновление базы данных признаков вредоносных компьютерных программ (вирусов) предусматривает:

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

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

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

3.4 В случае невозможности автоматического обновления базы данных признаков вредоносных компьютерных программ необходимо осуществить обновление вручную в соответствии с инструкцией разработчика антивирусного средства.