# ТИПОВОЙ ПОРЯДОК
## антивирусного контроля

### 1. Перечень используемых определений, обозначений и сокращений

АИБ – администратор информационной безопасности.
АРМ – автоматизированное рабочее место.
ИС – информационная система.
Администратор информационной безопасности – специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в ИС и на АРМ пользователей, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления несанкционированного доступа к защищаемой информации.

### 2. Общие положения

2.1. Настоящий Порядок определяет требования к организации защиты в информационных системах общего пользования, государственных информационных системах, информационных системах персональных данных, информационных системах, содержащих другие виды конфиденциальной информации, за исключением систем, содержащих сведения, составляющие государственную тайну, и систем, относящихся к ключевым системах информационной инфраструктуры (далее по тексту – ИС, защищаемые информационные ресурсы) организации, от разрушающего воздействия компьютерных вирусов.
2.2. К использованию в организации допускаются только лицензионные и сертифицированные антивирусные средства.
2.3. Установку и настройку параметров средств антивирусного контроля осуществляет АИБ в соответствии руководствами по применению конкретных антивирусных средств.

### 3. Применение средств антивирусного контроля

3.1. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должно проводиться обновление антивирусных баз через сеть Интернет с сайта разработчика антивирусных средств или любым доступным способом.

3.2. На всех включенных рабочих станциях должен работать в фоновом режиме Антивирус монитор для обеспечения автоматического контроля файловых операций.

3.3. Еженедельно и в автоматическом режиме должна проводится полная проверка всех файлов ИС и АРМ пользователей.

3.4. Для пользователя АРМ должна быть исключена возможность отключения средств антивирусной защиты, в том числе и его отдельных функций.

3.5. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

3.6. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов на серверах должны проводиться не реже одного раза в месяц.

3.7. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие программ вирусов и других вредоносных модулей. Непосредственно после установки (изменения) программного обеспечения рабочих станций и серверов ИС должна быть выполнена антивирусная проверка:

- на защищаемых серверах и АРМ;
- на других серверах и АРМ ИС, не требующих защиты, - лицом, установившим (изменившим) программное обеспечение.

3.8. 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.) сотрудник самостоятельно должен провести антивирусный контроль своей рабочей станции антивирусным сканером. При необходимости – привлечь АИБ для определения ими факта наличия или отсутствия компьютерного вируса.

3.9. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов АИБ, владельца зараженных файлов, а также сотрудников организации, использующих эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.