|  |  |
| --- | --- |
|  | Приложение 16  к приказу комитета  по культуре города Барнаула  от 29 июля 2021г. №64 |

ИНСТРУКЦИЯ

по проведению антивирусного контроля в информационных системах

Перечень используемых определений, обозначений и сокращений

АИБ – администратор информационной безопасности.

АРМ – автоматизированное рабочее место.

КИ – конфиденциальная информация.

ИС – информационная система.

ГИС – государственная информационная система.

НСД – несанкционированный доступ.

ПО – программное обеспечение.

Администратор информационной безопасности – специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в ИС, в том числе ИСПДн, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

1. Общие положения

1.1. Инструкция по проведению антивирусного контроля в информационных системах (далее – Инструкция) определяет требования к организации защиты в ИС общего пользования, ГИС, ИСПДн, ИС, содержащих другие виды КИ, за исключением систем, содержащих сведения, составляющие государственную тайну, и систем, относящихся к ключевым системах информационной инфраструктуры (далее – ИС) комитета по культуре города Барнаула (далее – комитет), от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих ИС за их выполнение.

1.2. К использованию в комитете допускаются только лицензионные и сертифицированные антивирусные средства.

1.3. Изменение используемого антивирусного средства необходимо согласовать с АИБом. Установка средств антивирусного контроля на рабочих станциях и серверах ИС осуществляется АИБом соответствии с «Инструкция по техническому обслуживанию, ремонту, модернизации технических средств, входящих в состав информационных систем комитета по культуре города Барнаула». Настройка параметров средств антивирусного контроля осуществляется АИБом в соответствии руководствами по применению конкретных антивирусных средств.

2.Применение средств антивирусного контроля

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

2.2. На всех включенных рабочих станциях средство антивирусной защиты должно работать в фоновом режиме.

2.3. 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 (магнитных дисках, лентах, CD-ROM и т. п.). 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).

2.4. 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 АИБом.

2.5. Устанавливаемое (изменяемое) ПО должно быть предварительно проверено АИБом на отсутствие программ вирусов и других вредоносных модулей. Непосредственно после установки (изменения) ПО рабочих станций и серверов ИС должна быть выполнена антивирусная проверка:

на защищаемых серверах и АРМ – АИБом;

на других серверах и АРМ ИС, не требующих защиты, – администратором ИС.

2.6. 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 АИБа для определения ими факта наличия или отсутствия компьютерного вируса.

2.7. 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 АИБа, владельца зараженных файлов, а также сотрудников комитета, использующих эти файлы в работе;

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

провести лечение или уничтожение зараженных файлов.

3. Ответственность

3.1. Ответственность за организацию антивирусного контроля в подразделении, эксплуатирующем ИС, в соответствии с требованиями настоящей Инструкции возлагается на АИБа.

3.2. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на всех сотрудников комитета, являющихся пользователями ИС.

3.3. Периодический контроль за состоянием антивирусной защиты в ИС комитете, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками комитета осуществляется АИБом.