|  |
| --- |
| Приложение 2 к Положению об обеспечении безопасности общедоступной информации в информационных системах комитета по финансам, налоговой и кредитной политике города Барнаула |

Порядок

проведения антивирусного контроля

1. Перечень используемых определений, обозначений и сокращений

АИБ – администратор информационной безопасности.

АРМ – автоматизированное рабочее место.

ИС – информационная система.

НСД – несанкционированный доступ.

ПО – программное обеспечение.

Администратор информационной безопасности – специалист отдела внедрения автоматизированных систем финансовых расчетов, осуществляющий контроль за обеспечением защиты информации в ИС, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

1. Общие положения
	1. Настоящий Порядок определяет требования к организации антивирусной защиты в информационных системах комитета по финансам, налоговой и кредитной политике города Барнаула, за исключением систем, содержащих сведения, составляющие государственную тайну, и систем, относящихся к ключевым системам информационной инфраструктуры (далее по тексту – ИС, защищаемые информационные ресурсы), от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих ИС за их выполнение.
	2. К использованию в комитете по финансам, налоговой и кредитной политике города Барнаула допускаются только лицензионные и сертифицированные антивирусные средства.
	3. Изменение используемого антивирусного средства необходимо согласовать с АИБом. Установка средств антивирусного контроля на рабочих станциях и серверах ИС осуществляется АИБом соответствии с Порядком обслуживания, ремонта, модернизации технических средств, входящих в состав информационных систем комитета по финансам, налоговой и кредитной политике города Барнаула. Настройка параметров средств антивирусного контроля осуществляется АИБом в соответствии руководствами по применению конкретных антивирусных средств.
2. Применение средств антивирусного контроля
	1. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должно проводиться обновление антивирусных баз любым доступным способом.
	2. Антивирусный контроль запускается в автоматическом режиме и осуществляется беспрерывно.
	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).
	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.
	5. Устанавливаемое (изменяемое) ПО должно быть предварительно проверено 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, - лицом, установившим (изменившим) программное обеспечение.
	1. 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 им факта наличия или отсутствия компьютерного вируса.
	2. 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 по финансам, налоговой и кредитной политике города Барнаула, использующих эти файлы в работе;
* совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
* провести лечение или уничтожение зараженных файлов.
1. Ответственность
	1. Ответственность за организацию антивирусного контроля в подразделении, эксплуатирующем ИС, в соответствии с требованиями настоящего порядка возлагается на АИБа.
	2. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящего Порядка возлагается на всех сотрудников комитета по финансам, налоговой и кредитной политике города Барнаула, являющихся пользователями ИС.
	3. Периодический контроль за состоянием антивирусной защиты в ИС комитета по финансам, налоговой и кредитной политике города Барнаула, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящего порядка сотрудниками комитета по финансам, налоговой и кредитной политике города Барнаула осуществляется АИБом.