УТВЕРЖДАЮ
<Председатель администрации>
_____/<Монгуш К.К. >
«21» декабря 2020г.

ИНСТРУКЦИЯ
по организации антивирусной защиты в государственных информационных системах в Администрации Пий-Хемского кожууна

1. Общие положения

1.1. Настоящая Инструкция определяет требования к организации защиты объектов информатизации от разрушающего воздействия компьютерных вирусов и устанавливает ответственность сотрудников Администрации Пий-Хемского кожууна, эксплуатирующих и сопровождающих ГИС, за их выполнение.

1.2. К использованию в ГИС допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств и прошедшие в установленном порядке процедуру оценки соответствия требованиям по безопасности.

1.3. После установки и настройки средств антивирусного контроля в обязательном порядке должно быть произведено тестирование системы антивирусной защиты.

1.4. Ответственность за организацию и проведение мероприятий антивирусного контроля возлагается на начальника отдела информационной политики Анай-оол Э.Б.

1.5. Ответственность за ежедневный антивирусный контроль в процессе эксплуатации ИС организации и своевременное информирование руководителя подразделения в случае обнаружения действий вредоносных программ возлагается на пользователей ИС.

2. Применение средств антивирусной защиты

2.1. В ГИС должна обеспечиваться антивирусная защита, 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 в ГИС должна предусматривать:

– применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), и иных точках доступа в информационную систему, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы);

– установку, конфигурирование и управление средствами антивирусной защиты;

– предоставление доступа средствам антивирусной защиты к объектам информационной системы, которые должны быть подвергнуты проверке средством антивирусной защиты;

– проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов);

– проверку в масштабе времени, близком к реальному, 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;

– оповещение администраторов безопасности в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов);

– определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами).

2.3 В информационной системе должно обеспечиваться предоставление прав по управлению (администрированию) средствами антивирусной защиты администратору безопасности.

2.4 В информационной системе должно обеспечиваться централизованное управление (установка, удаление, обновление, конфигурирование и контроль актуальности версий программного обеспечения средств антивирусной защиты) средствами антивирусной защиты, установленными на компонентах информационной системы (серверах, автоматизированных рабочих местах);

2.5 В ИС должно быть обеспечено обновление базы данных признаков вредоносных компьютерных программ (вирусов).

2.6 Обновление базы данных признаков вредоносных компьютерных программ (вирусов) должно предусматривать:

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

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

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

В информационной системе должно обеспечиваться централизованное управление обновлением базы данных признаков вредоносных компьютерных программ (вирусов).

2.7 Ежедневно в начале работы при загрузке компьютеров в автоматическом режиме должен проводиться антивирусный контроль всех электронных носителей информации, подключаемых к ИС.

2.8 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях.

2.9 Настройка средств антивирусной защиты должна реализовывать следующие функции:

– непрерывный автоматический мониторинг информационного обмена в ИС с целью выявления программно-математического воздействия;

– автоматическую проверку на наличие вредоносных программ или последствий программно-математических воздействий при импорте в ИС всех программных модулей (прикладных программ), которые могут содержать вредоносные программы;

– реализацию механизма автоматического блокирования обнаруженных вредоносных программ путем их удаления из программных модулей или уничтожения;

– полную автоматическую проверку носителей информации всех автоматизированных рабочих мест и серверов не реже одного раза в неделю;

– регулярное обновление антивирусных баз и программных модулей средств антивирусной защиты;

– автоматическое документирование состояния системы антивирусной защиты ИС.

2.10. Пользователи ИС при работе со съемными носителями информации обязаны перед началом работы осуществить их проверку на предмет отсутствия вредоносных программ, выполнив следующие действия:

– подключить съемный носитель информации;

– открыть значок Рабочего стола "Мой компьютер";

– установить курсор мыши на имя выбранного носителя;

– нажав на правую клавишу мыши открыть контекстное меню и выбрать пункт, запускающий антивирусную проверку электронного носителя информации.

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

2.12. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, появление сообщений о системных ошибках и т.п.) пользователь ИС должен обратиться к администратору ИС.

2.13. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи ИС обязаны:

– приостановить работу в ИС;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя подразделения, администратора ИС и других сотрудников, использующих эти файлы в работе.

2.14. Пользователь обязан осуществлять проверку файлов, получаемых:

– по электронной почте;

– через сеть интернет;

– на магнитном, оптическом диске, флеш–накопителе;

– ином съемном носителе информации;

– – полученные иным способом.

2.15. Пользователю запрещается:

– осуществлять действия, направленные на выключение антивирусной программы;

– самостоятельно устанавливать на АРМ программное обеспечение.

– запускать файлы, полученные по сетям связи (электронной почте, интернет), со съемных носителей, даже если они получены проверенного адресата, без предварительной их проверки антивирусной программой.