

УТВЕРЖДАЮ

“ ___ ” _____ 2018 года

ИНСТРУКЦИЯ ПО Компании АНТИВИРУСНОЙ ЗАЩИТЫ

Настоящая Инструкция определяет требования к организации защиты от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих АС Компании, за их выполнение.

К использованию в Компании допускаются только лицензионные антивирусные средства, централизованно закупленные (наименование подразделения _____) у разработчиков (поставщиков) указанных средств, рекомендованные к применению _____ отделом.

В случае необходимости использования антивирусных средств, не вошедших в перечень рекомендованных, их применение необходимо согласовать с _____ отделом Компании.

Установка средств антивирусного контроля на компьютерах (серверах ЛВС АС Компании) осуществляется уполномоченными сотрудниками отдела _____ в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы Компании». Настройка параметров средств антивирусного контроля осуществляется сотрудниками отдела _____ в соответствии руководствами по применению конкретных антивирусных средств.

Применение средств антивирусного контроля

Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС - при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов РС.

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 на выделенном автономном компьютере или, при условии начальной загрузки операционной системы в оперативную память компьютера с заведомо "чистой" (не зараженной вирусами) и защищенной от записи системной дискеты, - на любом другом компьютере. 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).

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

Установка (изменение) системного и прикладного программного обеспечения осуществляется на основании «Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы Компании». Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено отделом _____ на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной

сети), должна быть выполнена антивирусная проверка:

- на защищаемых серверах и РС - ответственным за обеспечение информационной безопасности;

- на других серверах и РС АС Компании не требующих защиты, - лицом, установившим (изменившим) программное обеспечение, - в присутствии и под контролем руководителя данного подразделения или сотрудника, им уполномоченного.

Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале подразделения за подписью лица, установившего (изменившего) программное обеспечение, и лица, его контролировавшего.

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 подразделения самостоятельно или вместе с ответственным за обеспечение безопасности информации подразделения (технологического участка) должен провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлечь специалистов отдела _____ для определения ими факта наличия или отсутствия компьютерного вируса.

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

- приостановить работу;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и ответственного за обеспечение информационной безопасности своего подразделения, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

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

- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов отдела _____);

- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на гибком магнитном диске в отдел _____ для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку (при необходимости, для выполнения требований данного пункта привлечь специалистов отдела _____);

- по факту обнаружения зараженных вирусом файлов составить служебную записку в отдел _____ (службу обеспечения безопасности информации), в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

Ответственность

Ответственность за организацию антивирусного контроля в подразделении, эксплуатирующем АС Организации, в соответствии с требованиями настоящей Инструкции возлагается на руководителя подразделения.

Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение безопасности информации и всех сотрудников подразделения, являющихся пользователями АС Компании.

Периодический контроль за состоянием антивирусной защиты в АС Компании, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками подразделений Компании осуществляется отделом _____

(службой обеспечения безопасности информации).