

Инструкция о применении средств антивирусной защиты информации

1. Термины и определения

В Инструкции о применении средств антивирусной защиты информации (далее - Инструкция) использованы следующие термины и определения:

Пользователи - должностные лица, а также все другие лица и организации, использующие в работе средства электронно-вычислительной техники.

Администраторы антивирусной защиты информации (далее - администраторы АВЗ) - должностные лица подразделений информационной безопасности (технических подразделений), назначенные ответственными за эксплуатацию средств антивирусной защиты информации и обеспечивающие организацию и эффективное использование системы антивирусной защиты информации.

Локально-вычислительная сеть (далее - ЛВС) - группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными (неарендуемыми) высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

Антивирусная защита информации - система организационно-технических мероприятий, требований и условий использования электронно-вычислительной техники, предназначенная для предотвращения заражения программными вирусами информационно-вычислительных ресурсов посредством применения средств антивирусной защиты информации.

Вредоносная программа - программа для электронно-вычислительных машин (ЭВМ), заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети.

Программные вирусы - разновидность вредоносных программ, отличительной особенностью которых является способность к размножению (саморепликации). В дополнение к этому они могут повреждать или полностью уничтожать данные, подконтрольные пользователю, от имени которого была запущена зараженная программа.

Информационно-техническая служба - структурное подразделение организации, ответственное за функционирование автоматизированных информационных систем и электронно-вычислительной техники. В небольших организациях на него могут быть возложены и функции службы информационной безопасности.

2. Общие положения

1. Настоящая Инструкция разработана в целях осуществления антивирусной защиты информации, содержащейся и обрабатываемой на рабочих станциях структурных подразделений организации, от несанкционированного копирования, модификации и разрушения данных, используемых в деятельности учреждения, а также нарушения работы используемого программного обеспечения при воздействии вирусов и других вредоносных программ посредством комплекса организационно-технических мероприятий по обеспечению информационной безопасности.

2. Настоящая Инструкция определяет порядок применения средств антивирусной защиты в структурных подразделениях, задачи, обязанности и права администраторов АВЗ, пользователей средств антивирусной защиты информации, порядок установки и применения обновлений, подключения средств антивирусной защиты, а также порядок ликвидации последствий воздействия программных вирусов.

3. Требования настоящей Инструкции обязательны для выполнения всеми пользователями и администраторами АВЗ, а также иными лицами, использующими средства вычислительной техники.

4. Общее руководство обеспечением антивирусной защиты информации в осуществляется информационно-технической службой (далее - ИТС) и ответственным за информационную безопасность и техническую защиту информации ИТС.

5. Ответственный за информационную безопасность и техническую защиту информации ИТС осуществляет непосредственное руководство организацией проведения работ по антивирусной защите информации в организации через сотрудников ИТС.

6. Практическое решение задач, связанных с организацией антивирусной защиты информации и применением средств антивирусной защиты информации в структурных подразделениях, осуществляется сотрудниками ИТС.

7. При возникновении ситуаций, не включенных в положения настоящей Инструкции, решение принимается администратором АВЗ по согласованию с ответственным за информационную безопасность и техническую защиту информации ИТС.

3. Порядок применения средств антивирусной защиты информации в образовательном учреждении

1. Средства антивирусной защиты информации должны устанавливаться на всех средствах вычислительной техники, эксплуатируемых в образовательном учреждении. При технологической необходимости на отдельные средства вычислительной техники средства антивирусной защиты информации могут не устанавливаться. Список таких исключений утверждается руководителем ИТС и пересматривается ежегодно.

2. Порядок применения средств антивирусной защиты информации устанавливается с учетом соблюдения следующих требований:

- обязательный входной контроль за отсутствием программных вирусов во всех поступающих на объект информатизации электронных носителях информации, информационных массивах, программных средствах общего и специального назначения;

- обязательная проверка всех электронных писем на предмет отсутствия программных вирусов;

- периодическая проверка на предмет отсутствия программных вирусов жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка съемных носителей информации перед началом работы с ними;

- внеплановая проверка жестких магнитных дисков и съемных носителей информации в случае подозрения на наличие программных вирусов;

- восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами.

3. Уполномоченное лицо организации по антивирусной защите информации обеспечивает:

- управление конфигурацией и логической структурой всего программного обеспечения системы антивирусной защиты информации;

- управление установкой и обновлением лицензионных ключей средств антивирусной защиты информации;

- управление рассылкой и установкой обновлений баз средств антивирусной защиты информации;

- ограничение доступа пользователей на рабочих местах к настройкам установленных средств антивирусной защиты информации;

- настройку рассылки сообщений об обнаружении вирусов, о сбоях в работе средств антивирусной защиты и т.п.;

- удаленное решение проблем, возникающих в процессе использования средств антивирусной защиты информации.

4. Для рабочих станций и серверов, которые не имеют подключения к ЛВС, средства антивирусной защиты информации для них устанавливаются локально в порядке, определенном администратором АВЗ, с учетом требований настоящей Инструкции.

5. Установка и настройка средств антивирусной защиты информации осуществляются в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.

6. Копирование любой информации, переносимой с помощью любых съемных носителей информации, должно производиться только после проведения процедуры полного антивирусного контроля съемного носителя. 7. Антивирусная профилактика является необходимым элементом защиты информационных ресурсов учреждения от их модификации и уничтожения. Антивирусная профилактика состояния средств антивирусной защиты информации на серверах и рабочих станциях должна проводиться по согласованию с администраторами АВЗ в нерабочее время, за исключением внештатных ситуаций.

4. Порядок обновления баз данных средств антивирусной защиты информации

1. Своевременное обновление баз данных средств антивирусной защиты информации в структурных подразделениях является неотъемлемой частью обеспечения эффективной политики антивирусной защиты информации.

2. Обновление баз данных средств антивирусной защиты информации на рабочих станциях, установленных локально в структурных подразделениях, должно производиться не реже одного раза в неделю в порядке, устанавливаемом администратором АВЗ, с учетом требований настоящей Инструкции.

3. На рабочем месте администратора АВЗ могут быть установлены средства, позволяющие через ЛВС управлять компонентами системы антивирусной защиты, установленными на рабочих станциях и серверах в структурных подразделениях, а также проводить обновления баз средств антивирусной защиты информации. В случае если рабочая станция пользователя не подключена к ЛВС, обновление средств антивирусной защиты информации производится пользователем через съемные носители информации. Периодичность обновления определяется программными требованиями средств антивирусной защиты информации или устанавливается администратором АВЗ.

5. Обязанности, права и порядок назначения администраторов АВЗ

1. Администраторы АВЗ обязаны обеспечивать соблюдение в учреждении политики антивирусной защиты информации и выявление фактов заражения программными вирусами.

2. К основным задачам администратора АВЗ относятся организация процесса установки и обновления средств антивирусной защиты информации на рабочих станциях пользователей и обеспечение технического сопровождения действий пользователей в случаях обнаружения программных вирусов, а также осуществление контроля за состоянием системы антивирусной защиты информации.

3. Администратор АВЗ несет ответственность: за своевременную установку средств антивирусной защиты информации;

- за эксплуатацию системы антивирусной защиты информации;
- за своевременное обновление лицензий на средства антивирусной защиты информации;

- за своевременное обновление баз данных средств антивирусной защиты информации.

4. Администратор АВЗ имеет право:

- вносить предложения по совершенствованию системы антивирусной защиты информации в структурных подразделениях образовательного учреждения;

- принимать участие в планировании мероприятий по антивирусной защите информации в организации и планировании оснащения средствами антивирусной защиты информации структурных подразделений;

- осуществлять контроль состояния средств антивирусной защиты информации в структурных подразделениях;

- проводить служебные проверки по фактам заражения программными вирусами автоматизированных систем обработки информации и средств вычислительной техники в структурных подразделениях образовательного учреждения;

- оказывать помощь в решении проблем, возникающих при эксплуатации средств антивирусной защиты информации в структурных подразделениях образовательного учреждения.

5. Назначение администраторов АВЗ организации осуществляется на основании приказа по образовательному учреждению с обязательным отражением обязанностей в должностной инструкции.

6. Обязанности администраторов АВЗ могут совмещать должностные лица, назначенные администраторами баз данных (автоматизированных информационных систем), специалисты ИТС. Администраторами АВЗ не могут быть должностные лица сторонних организаций. Должностные лица, исполняющие обязанности администраторов АВЗ, утверждается приказом руководителя образовательного учреждения.

7. Обязанности администраторов АВЗ организации другие лица могут исполнять только на основании приказа руководителя организации о временном исполнении обязанностей администратора АВЗ, в котором указан срок исполнения обязанностей администратора АВЗ.

6. Обязанности пользователей средств антивирусной защиты информации

1. Пользователь обязан изучить настоящую Инструкцию и ознакомиться с необходимостью несения ответственности за выполнение ее требований под роспись.

2. Пользователям запрещается:

- отключать средства антивирусной защиты информации во время работы;

- использовать средства антивирусной защиты информации, отличные от поддерживаемых ИТС, перечень которых доводится до сведения пользователей ИТС или администраторов АВЗ;

- без разрешения администратора ЛВС и администратора АВЗ копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

3. Ввод информации с магнитных, оптических, магнитооптических и любых других съемных носителей информации неслужебного характера должен осуществляться пользователем только с разрешения администраторов ЛВС или администраторов АВЗ.

4. В случае появления подозрений на наличие программных вирусов в ЛВС пользователи должны немедленно проинформировать об этом администратора АВЗ. В случае выявления инцидентов (фактов и т.п.), связанных со сбоями в работе средств

антивирусной защиты, пользователь обязан незамедлительно сообщить об этом ответственному за информационную безопасность и техническую защиту информации ИТС.

7. Порядок действий пользователей и администраторов АВЗ при обнаружении вирусов

1. Основными путями проникновения вирусов в информационно - вычислительную сеть организации являются: гибкие магнитные диски, компакт-диски, иные съемные накопители информации, электронная почта, файлы, получаемые из сети Интернет, ранее зараженные рабочие станции. В случае обнаружения программных вирусов при входном контроле отчуждаемых носителей информации, файлов или почтовых сообщений, поступивших в структурные подразделения, пользователь должен:

- приостановить процесс приема-передачи информации;
- сообщить администратору АВЗ или ответственному за информационную безопасность и техническую защиту информации ИТС о факте обнаружения программного вируса;
- принять по согласованию с администратором АВЗ меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации;
- сообщить о факте обнаружения программного вируса в структурное подразделение, из которого поступили зараженные съемные электронные носители информации, файлы или почтовые сообщения.

2. При обнаружении программных вирусов в процессе обработки информации пользователь обязан:

- немедленно приостановить все работы;
- сообщить администратору АВЗ или ответственному за информационную безопасность и техническую защиту информации ИТС о факте обнаружения программных вирусов;
- принять по согласованию с администратором АВЗ меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации.

3. Программные средства общего и специального назначения, используемые в структурных подразделениях для обработки информации, отнесенной к служебной тайне, в случае обнаружения программных вирусов подлежат обязательной переустановке с рабочих копий эталона.

4. При невозможности ликвидации последствий заражения программными вирусами администратору АВЗ необходимо:

- заархивировать зараженные файлы с внедренными программными вирусами и направить с приложением соответствующего сопроводительного документа в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации;
- осуществить полную переустановку программного обеспечения на зараженном компьютере.

5. При получении информации о возможном нарушении либо выявлении факта нарушения требований настоящей Инструкции работа на рабочей станции данного пользователя незамедлительно блокируется по решению администратора АВЗ.

6. Все факты модификации и разрушения данных на серверах или рабочих станциях, заражение их вирусами, а также обнаружение других вредоносных программ классифицируются как значимые нарушения информационной безопасности и должны анализироваться посредством проведения служебного расследования, проводимого по приказу руководителя образовательного учреждения.

8. Ответственность за выполнение требований Инструкции

1. За нарушение настоящей Инструкции администратор АВЗ и пользователи несут ответственность, установленную действующим законодательством Российской Федерации и нормативными правовыми актами.

2. Руководители структурных подразделений несут ответственность за выполнение мероприятий по антивирусной защите информации на средствах вычислительной техники, эксплуатируемых подчиненными должностными лицами, и за ознакомление их (под роспись) с настоящей Инструкцией в своем структурном подразделении.

3. Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации на своих рабочих местах, в том числе за своевременное обновление антивирусных баз средств антивирусной защиты информации и получение новых лицензионных ключей, несут пользователи, за которыми закреплены средства вычислительной техники.

4. В случае нарушения требований настоящей Инструкции, связанных с применением пользователем средств антивирусной защиты информации, пользователь несет персональную ответственность, установленную действующим законодательством Российской Федерации и локальными нормативными актами образовательного учреждения.

5. Ответственность за выполнение требований настоящей Инструкции администраторами АВЗ несут непосредственно администраторы АВЗ и руководители подразделений, в которых работают администраторы АВЗ.

9. Порядок оснащения организации средствами антивирусной защиты информации

1. Оснащение средствами антивирусной защиты информации является видом материального обеспечения и осуществляется в образовательном учреждении централизованно.

2. Передача полученных средств антивирусной защиты на объекты, не входящие в состав организации, запрещена. За несанкционированное распространение средств антивирусной защиты информации виновные несут ответственность в соответствии с законодательством Российской Федерации.