ПРИЛОЖЕНИЕ № 2
УТВЕРЖДЕНА
распоряжением администрации
Знаменского муниципального округа
от 22.01.2024 № 24-р

Инструкция
по проведению антивирусного контроля в ИСПДн администрации Знаменского муниципального округа Тамбовской области

1. Общие положения

1.1 Настоящая Инструкция разработана в целях осуществления антивирусной защиты информации, содержащейся и обрабатываемой на рабочих станциях ИСПДн администрации Знаменского муниципального округа Тамбовской области и ЛВС, от несанкционированного копирования, модификации и разрушения, а также нарушения работы используемого программного обеспечения при воздействии вирусов и других вредоносных программ посредством комплекса организационно-технических мероприятий по обеспечению информационной безопасности.

1.2 Настоящая Инструкция определяет порядок применения средств антивирусной защиты, задачи, обязанности и права Администратора безопасности, пользователей средств антивирусной защиты информации, порядок установки и применения обновлений, а также порядок ликвидации последствий воздействия программных вирусов.

1.3 Требования настоящей Инструкции обязательны для выполнения пользователями ИСПДн и Администратором безопасности, а также иными лицами, использующими средства вычислительной техники.

1.4 Практическое решение задач, связанных с организацией антивирусной защиты информации и применением средств антивирусной защиты, осуществляется Администратором безопасности.

2. Порядок применения средств антивирусной защиты информации

2.1 Средства антивирусной защиты информации должны устанавливаться на всех автоматизированных рабочих местах Администрации Знаменского муниципального округа Тамбовской области, обрабатывающих персональные данные.

2.2 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.

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

2.4 Копирование любой информации, переносимой с помощью любых съемных носителей информации, должно производиться только после проведения процедуры полного антивирусного контроля съемного носителя.

2.5 Антивирусная профилактика является необходимым элементом защиты информационных ресурсов от их модификации и уничтожения. Антивирусная профилактика состояния средств антивирусной защиты информации на серверах и рабочих станциях должна, как правило, проводиться по согласованию с Администратором безопасности.

2.6 Своевременное обновление баз данных средств антивирусной защиты информации является неотъемлемой частью обеспечения эффективной политики антивирусной защиты информации.

2.7 Обновление баз данных средств антивирусной защиты информации на рабочих станциях и серверах в ЛВС осуществляется в автоматическом режиме.

2.8 На рабочем месте Администратора безопасности могут быть установлены средства, позволяющие через ЛВС управлять компонентами системы антивирусной защиты, установленными на рабочих станциях и серверах, 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 безопасности.

3. Обязанности и права Администратора безопасности

3.1 Администратор безопасности обязан обеспечивать соблюдение политики антивирусной защиты информации и выявление фактов заражения программными вирусами.

3.2 К основным задачам Администратора безопасности 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.

3.3 Администратор безопасности 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.

3.4 Администратор безопасности имеет право:
– осуществлять контроль состояния средств антивирусной защиты;
– проводить служебные проверки по фактам заражения программными вирусами автоматизированных систем обработки информации и средств вычислительной техники;
– оказывать помощь в решении проблем, возникающих при эксплуатации средств антивирусной защиты информации.

4. Обязанности пользователей средств антивирусной защиты информации

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

4.2 Пользователям запрещается:
– отключать средства антивирусной защиты информации во время работы;
– без разрешения Администратора безопасности копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

4.3 В случае появления подозрений на наличие программных вирусов в ЛВС пользователи должны немедленно проинформировать об этом Администратора безопасности. В случае выявления инцидентов (фактов и т.п.), связанных со сбоями в работе средств антивирусной защиты, пользователь обязан незамедлительно сообщить об этом администратору безопасности.

5. Порядок действий пользователей и Администратора безопасности при обнаружении вирусов

5.1 В случае обнаружения программных вирусов при входном контроле отчуждаемых носителей информации, файлов или почтовых сообщений пользователь должен:
– приостановить процесс приема-передачи информации;
– сообщить Администратору безопасности о факте обнаружения программного вируса;
– принять по согласованию с Администратором безопасности меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации.

5.2 При обнаружении программных вирусов в процессе обработки информации пользователь обязан:
– немедленно приостановить все работы;
– сообщить Администратору безопасности о факте обнаружения

программных вирусов;

– принять по согласованию с Администратором безопасности меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации.

5.3 При невозможности ликвидации последствий заражения программными вирусами Администратору безопасности необходимо:

– сообщить в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации;

– заархивировать зараженные файлы с внедренными программными вирусами и направить в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации;

– осуществить полную переустановку программного обеспечения на зараженном компьютере.

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

5.5 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.

6. Ответственность за выполнение требований Инструкции

6.1 За нарушение настоящей Инструкции Администратор безопасности и пользователи несут ответственность, установленную действующим законодательством Российской Федерации и нормативными правовыми актами.

6.2 Начальник отдела информатизации администрации Знаменского муниципального округа несет 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.

6.3 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.

6.4 В случае нарушения требований настоящей Инструкции, связанных с применением пользователем средств антивирусной защиты информации, пользователь несет персональную ответственность, установленную действующим законодательством Российской Федерации и нормативно правовыми актами.

6.5 Ответственность за выполнение требований настоящей Инструкции несет Администратор безопасности.

7. Порядок оснащения средствами антивирусной защиты информации

7.1 Оснащение средствами антивирусной защиты информации является видом материального обеспечения и осуществляется централизованно.

7.2 За несанкционированное распространение средств антивирусной защиты информации виновные несут ответственность в соответствии с законодательством Российской Федерации.

8. Порядок информирования о вирусной активности

8.1 Своевременное информирование о вирусной активности является составной частью системы антивирусной защиты информации.

8.2 Информирование (распространение предупреждений) о вирусной активности осуществляется централизованно через электронную почту посредством автоматической рассылки или иным способом по усмотрению Администратора безопасности.