УТВЕРЖДЕНА
Приказом заведующего
МБДОУ «Детский сад №1 г. Выборга»
от 19.05.2025г. № 91

ИНСТРУКЦИЯ
О ПРИМЕНЕНИИ СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ В МБДОУ «ДЕТСКИЙ САД №1 Г. ВЫБОРГА»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция о применении средств антивирусной защиты информации разработана в целях осуществления антивирусной защиты информации, содержащейся и обрабатываемой в МБДОУ «Детский сад №1 г.Выборга» (далее по тексту ДОУ), от несанкционированного копирования, модификации и разрушения данных, используемых в деятельности ДОУ, 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 в структурных подразделениях, задачи, обязанности и права администраторов, пользователей средств антивирусной защиты информации, порядок установки и применения обновлений, подключения средств антивирусной защиты, а также порядок ликвидации последствий воздействия программных вирусов.

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

1.4. Ответственный за информационную безопасность осуществляет непосредственное руководство организацией проведения работ по антивирусной защите информации в ДОУ.

1.5. При возникновении ситуаций, не включенных в положения настоящей Инструкции, решение принимается администратором по согласованию с заведующим ДОУ.

2. ПОРЯДОК ПРИМЕНЕНИЯ СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ

2.1. Средства антивирусной защиты информации должны устанавливаться на всех средствах вычислительной техники, эксплуатируемых в ДОУ. При технологической необходимости на отдельные средства вычислительной техники средства антивирусной защиты информации могут не устанавливаться. Список таких исключений утверждается заведующим ДОУ и пересматривается ежегодно.

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 все 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. Ответственное лицо ДОУ по антивирусной защите информации (далее по тексту Администратор) 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.

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

2.5. Настройка средств антивирусной защиты информации осуществляются в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.

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

2.7. Антивирусная профилактика является необходимым элементом защиты информационных ресурсов ДОУ от их модификации и уничтожения. Антивирусная профилактика состояния средств антивирусной защиты информации на серверах и рабочих станциях должна проводиться по согласованию с администраторами в нерабочее время, за исключением внештатных ситуаций.

3. ПОРЯДОК ОБНОВЛЕНИЯ БАЗ ДАННЫХ СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

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

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

3.3. На рабочем месте администратора могут быть установлены средства, позволяющие управлять компонентами системы антивирусной защиты, установленными на рабочих станциях и серверах, а также проводить обновления баз средств антивирусной защиты информации. В случае если рабочего места пользователя не подключена, обновление средств антивирусной защиты информации производится пользователем через съемные носители информации. Периодичность обновления определяется

программными требованиями средств антивирусной защиты информации или устанавливается администратором.

4. ОБЯЗАННОСТИ, ПРАВА И ПОРЯДОК НАЗНАЧЕНИЯ АДМИНИСТРАТОРА

4.1. Администратор обязан обеспечивать соблюдение в ДОУ политики антивирусной защиты информации и выявление фактов заражения программными вирусами.

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

4.3. Администратор 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.

4.4. Администратор имеет право:

- вносить предложения по совершенствованию системы антивирусной защиты информации в ДОУ;
- принимать участие в планировании мероприятий по антивирусной защите информации в ДОУ 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 ДОУ;
- оказывать помощь в решении проблем, возникающих при эксплуатации средств антивирусной защиты информации в ДОУ.

4.5. Назначение администратора осуществляется на основании приказа заведующего ДОУ.

4.6. Обязанности администратора могут совмещать должностные лица, назначенные администраторами баз данных (автоматизированных информационных систем). Администратором не могут быть должностные лица сторонних организаций.

6. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

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

6.2. Пользователям запрещается:

- отключать средства антивирусной защиты информации во время работы;
- использовать средства антивирусной защиты информации, перечень которых доводится до сведения пользователей или администратора;
- без разрешения администратора копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

6.3. Ввод информации с магнитных, оптических, магнитооптических и любых других съемных носителей информации неслужебного характера должен осуществляться пользователем только с разрешения администратора.

6.4. В случае появления подозрений на наличие программных вирусов, пользователи должны немедленно проинформировать об этом администратора. В случае выявления инцидентов (фактов и т.п.).

7. ПОРЯДОК ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ И АДМИНИСТРАТОРА АВЗ ПРИ ОБНАРУЖЕНИИ ВИРУСОВ

7.1. 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 места. В случае обнаружения программных вирусов при входном контроле отчуждаемых носителей информации, файлов или почтовых сообщений, поступивших в ДОУ, пользователь должен:

- приостановить процесс приема-передачи информации;
- сообщить администратору о факте обнаружения программного вируса;
- принять по согласованию с администратором меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации;
- сообщить о факте обнаружения программного вируса, из которого поступили зараженные съемные электронные носители информации, файлы или почтовые сообщения.

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

- немедленно приостановить все работы;
- сообщить администратору о факте обнаружения программных вирусов;
- принять по согласованию с администратором меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации.

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

7.4. При невозможности ликвидации последствий заражения программными вирусами администратору 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.

7.5. При получении информации о возможном нарушении либо выявлении факта нарушения требований настоящей Инструкции работа на рабочем месте данного пользователя незамедлительно блокируется по решению администратора.

6. Все факты модификации и разрушения данных на серверах или рабочих мест, 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 заведующего ДОУ.

8. ОТВЕТСТВЕННОСТЬ ЗА ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ ИНСТРУКЦИИ

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

8.2. Администратор 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.

8.3. 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.

8.4. 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 ДОУ.

9. ПОРЯДОК ОСНАЩЕНИЯ ОРГАНИЗАЦИИ СРЕДСТВАМИ АНТИВИРУСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

9.1. Оснащение средствами антивирусной защиты информации является видом материального обеспечения и осуществляется в ДОУ.

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

С инструкцией ознакомлен (а), экземпляр инструкции получил(а).

«____»_____20___ г. _____/_____/