

**АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ**

**«ХОЛМ-ЖИРКОВСКИЙ РАЙОН» СМОЛЕНСКОЙ ОБЛАСТИ**

**Р А С П О Р Я Ж Е Н И Е**

от 25.05.2020 № 236-р

|  |  |
| --- | --- |
| Об утверждении инструкции по антивирусной защите информации в Администрации муниципального образования «Холм-Жирковский район» Смоленской области |  |

В соответствии с постановлением Администрации Смоленской области от 20.07.2015 № 424 «О порядке использования распределенной мультисервисной сети связи и передачи данных органов исполнительной власти Смоленской области и органов местного самоуправления муниципальных образований Смоленской области»:

1. Утвердить инструкцию по антивирусной защите информации в Администрации муниципального образования «Холм-Жирковский район» Смоленской области согласно приложению.

2. Специалисту I категории отдела по информационной политике Администрации муниципального образования «Холм-Жирковский район» Смоленской области (А.С. Морозов) обеспечивать соблюдение настоящей инструкции.

3. Настоящее распоряжение вступает в силу после дня подписания.

Глава муниципального образования

«Холм-Жирковский район»

Смоленской области **А.М. Егикян**

|  |
| --- |
| Приложениек распоряжению Администрации муниципального образования «Холм-Жирковский район» Смоленской области от 25.05.2020 № 236-р |

**ИНСТРУКЦИЯ**

**по организации антивирусной защиты информации**

**в** **Администрации муниципального образования**

**«Холм-Жирковский район» Смоленской области**

**1. Термины и их определения**

Приведенные в данном разделе термины и определения применяются в настоящей инструкции по организации антивирусной защиты информации в Администрации муниципального образования «Холм-Жирковский район» Смоленской области (далее и Инструкция) в следующих значениях:

- **автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

* **вирусная эпидемия** - нарушение нормального функционирования либо прекращение функционирования операционных систем компьютеров, в том числе не связанных между собой локальной сетью, возникающее в результате распространения программных вирусов и характеризующееся причинением материального ущерба;
* **вредоносная** **программа** – программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы:
* **информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
* **информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
* **программный вирус** - вредоносная программа, способная создавать свои копии или другие вредоносные программы, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации, либо копированию информации, нарушению работы автоматизированных систем.

**2. Общие положения**

2.1. Настоящая Инструкция определяет структуру системы антивирусной защиты информации и основы организации системы антивирусной защиты информации в Администрации района.

1. Настоящая Инструкция является документом, обязательным для исполнения при проведении работ по организации антивирусной защиты информации.
2. Настоящая Инструкция разработана в соответствии с нормативными документами Российской Федерации в области защиты информации.

**3. Система антивирусной защиты информации**

1. Система антивирусной защиты информации Администрации района является частью системы информационной безопасности и предназначена для предотвращения заражения программными вирусами информационных систем и рабочих мест пользователей.
2. Система антивирусной защиты информации Администрации района является комплексной системой, состоящей из совокупности организационных, правовых ипрограммно-аппаратных мер и средств, направленных на обеспечение эффективной антивирусной защиты информации в информационных системах Администрации района. Комплексность систем у антивирусной защитыдостигается контролем всех информационных потоков, протекающих в распределенной мультисервисной сети связи и передачи данных органов исполнительной власти Смоленской области и органов местного самоуправления муниципальных образований Смоленской области (далее РМС) и согласованием между собой разнородных методов и средств, обеспечивающих антивирусную защиту элементов РМС.
3. Функционирование системы антивирусной защиты РМС осуществляется в рамках работ по созданию и развитию системы информационной безопасности.
4. Руководство системой антивирусной защиты информации, обеспечение ее функционирования и обновления программного обеспечения осуществляет администратор информационной безопасности Администрации района, в том числе:
5. Планирование и оснащение Администрации района средствами антивирусной защиты.
6. Контроль состояния антивирусной защиты информации в Администрации района.
7. Анализ состояния и разработку предложений по совершенствованию системы антивирусной защиты информации.
8. Планирование мероприятий по антивирусной защите.
9. Осуществление мероприятий по антивирусной защите информации Администрации района.
10. При организации системы антивирусной защиты информации используется специализированное, сертифицированное по требования безопасности, программное обеспечение, допускающее дистанционное управление антивирусным программным обеспечением Администратором антивирусной защиты информации.
11. Инсталляция и настройка средств антивирусной защиты информации осуществляются в соответствии с программной и эксплуатационной документацией; поставляемой в комплекте с ними.
12. Практическое выполнение мероприятий по обеспечению антивирусной защиты информации осуществляет администратор информационной безопасности Администрации района, пользователи РМС.
13. Администратор антивирусной защиты информации обеспечивает:

- Обновление баз данных средств антивирусной защиты;

- Непрерывное функционирование сервера администрирования антивирусной защиты;

- Управление группами администрирования;

- Отслеживание вирусных эпидемий;

- Организацию ликвидации последствий заражения средств вычислительной техники программными вирусами.

3.9. Сотрудники, ответственные за обеспечение антивирусной защиты информации в Администрации района и подведомственных учреждениях обеспечивает:

- Инсталляцию и настройку средств антивирусной защиты информации на автоматизированных рабочих местах;

- Обновление баз данных средств антивирусной защиты информации на автоматизированных рабочих местах;

- Обучение пользователей правилам работы со средствами антивирусной защиты информации;

- Отслеживание вирусных эпидемий;

- Ликвидацию последствий заражения средств вычислительной техники программными вирусами.

**4. Применение средств антивирусной защиты**

4.1. Ежедневно, при загрузке компьютера, в автоматическом режиме проводится контроль целостности и антивирусный контроль системных областей жесткого диска компьютера.

1. Полная антивирусная проверка компьютера проводится не реже одного раза в месяц.
2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая на съемных носителях. Контроль исходящей информации необходимо проводить непосредственно перед записью на съемный носитель.
3. Устанавливаемое (изменяемое) на АРМ и серверах программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, должна быть выполнена полная антивирусная проверка.
4. Пользователю запрещается предпринимать действия по отключению или блокированию работы антивирусного программного обеспечения.

**5. Порядок обновления баз данных средств антивирусной защиты**

**информации**

5.1 Своевременное обновление баз данных средств антивирусной защиты информации являетсянеотъемлемой частьюобеспечения эффективной антивирусной защиты информации. Обновления антивирусных баз и активация лицензий антивирусного программного обеспечения, предоставляемого Департаментом Смоленской области по информационным технологиям (далее – Департамент) осуществляются Департаментом.

5.2. Обновление баз данных средств антивирусной защиты информацииосуществляется централизованно через серверы администрирования системы антивирусной защиты ежедневно, не реже одного раза в 4 часа, а для автоматизированных рабочих мест, не имеющих подключения к РМС еженедельно.

**6. Порядок информирования о вирусной активности**

6.1. Своевременное информирование пользователей РМС о вирусной активности является составной частью системы антивирусной защиты информации.

6.2 Информирование пользователей производится:

- Департаментом через ответственных за обеспечение антивирусной защиты в органах исполнительной власти и подведомственных им учреждениях;

- Ответственным за организацию работ по защите информации;

- Администратором информационной безопасности Администрации района.

6.3. При возникновении чрезвычайных ситуаций (вирусных эпидемий)
Администратор информационной безопасности Администрации района организует рассылку ответственным за обеспечение антивирусной защиты информации в подведомственных учреждениях рекомендаций по предотвращению заражений средств вычислительной техники программными вирусами.

**7. Действия при обнаружении программных вирусов**

7.1. В случае обнаружения программных вирусов при входном контролемашинных носителей информации, файлов или почтовых сообщений, поступивших в Администрации района, пользователь обязан прекратить процесс приема-передачи информации. Если входящая информация (носитель) поступила из внутренней сегмента РМС, пользователь обязан сообщить о факте обнаружения вирусов ответственному за обеспечение антивирусной защиты.

7.2. При обнаружении программных вирусов в процессе обработки информации:

- Пользователь обязан немедленно прекратить все работы со средствами вычислительной техники, по возможности, локализовать источник распространения вирусов и незамедлительно сообщить Администратору информационной безопасности Администрации района о факте обнаружения программного вируса.

- Администратор информационной безопасности обязан принять меры по локализации и удалению программных вирусов на рабочем месте пользователя, обеспечить ликвидацию последствий заражения.

7.3. При невозможности ликвидации последствий заражения программными вирусами Администратор информационной безопасности обязан:

- Сообщить о факте невозможности ликвидации последствий заражения Администратору антивирусной защитыинформации;

- Самостоятельно или с помощью Администратора антивирусной защиты информации сформировать архивные копии файлов с внедренными программными вирусами и направить их с приложением соответствующего сопроводительного документа в Департамент;

- При необходимости осуществить полную переустановку программного обеспечения персонального компьютера.

**8. Ответственность**

8.1. Администратор информационной безопасности несет ответственность за неисполнение (ненадлежащее исполнение) возложенных нанего обязанностей в рамках реализации мер по антивирусной защите информации.

8.2. Пользователи АРМ несут ответственность за обеспечение установленных норм антивирусной защиты информации насвоих рабочих местах.