**Муниципальное казенное учреждение**

**«Администрация Киндальского сельского поселения»**

**Каргасокского района Томской области**

**РАСПОРЯЖЕНИЕ**

12.09.2019 г. № 33

с. Киндал

|  |  |
| --- | --- |
| Об утверждении Положения об антивирусной политики в Администрации Киндальского сельского поселения |  |

В целях исполнения [Федерального закона](garantF1://12048567.0) от 27.07.2006 года № 152-ФЗ "О персональных данных", [Постановления Правительства Российской Федерации от 21.03.2012 г. № 211](http://itsec2012.ru/postanovlenie-ot-21-marta-2012-g-n-211) «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» в Администрации Киндальского сельского поселения:

# 1. Утвердить Положение об антивирусной политике в Администрации Киндальского сельского поселения согласно приложению к настоящему распоряжению.

2. Ведущему специалисту Администрации Киндальского сельского поселения ознакомить под роспись с настоящим распоряжением всех работников Администрации Киндальского сельского поселения, имеющих по роду своей деятельности доступ к информационным системам, в которых ведется автоматизированная обработка персональных данных.

3. Утратило силу Распоряжение № 87 от 14.12.2015 г. «Об утверждении Положения об антивирусной политики в Администрации Киндальского сельского поселения»

4. Контроль за исполнением данного Положения об антивирусной политике в Администрации Киндальского сельского поселения возложить на ведущего специалиста Администрации Киндальского сельского поселения.

Глава Киндальского

сельского поселения В.В.Волков

|  |  |
| --- | --- |
|  |  |

Ознакомлены:

1. Прытова О.Н.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Назипова А.В.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Кондейкина А.С.\_\_\_\_\_\_\_\_\_\_\_\_\_\_

УТВЕРЖДЕНО

# распоряжением Администрации

Киндальского сельского поселения от 12.09.2019 № 33

Приложение

Положение об антивирусной политике

в Администрации Киндальского сельского поселения

I.Общее положение

Вирус (компьютерный) – вредоносная программа, способная создавать свои копии или другие вредоносные программы и внедрять их в файлы, системные области компьютера, распространяться через компьютерные сети, а также осуществлять другие деструктивные действия.

Антивирус – программное средство, предназначенное для борьбы с вирусами, основными задачами которого является:

1) препятствие проникновению вирусов в компьютерную систему;

2) обнаружение вирусов в компьютерной системе;

3) устранение вирусов из компьютерной системы без нанесений повреждений другим объектам системы;

4) минимизация ущерба от действий вирусов.

Антивирусная защита (далее - АВЗ) – комплекс правовых, организационных и технических мер по защите от воздействия вредоносных программ (вирусов).

Антивирусное программное обеспечение – программное обеспечение (далее – АПО), предназначенное для защиты от вредоносных программ посредством обнаружения зараженных программных модулей и системных областей, распознания и блокировки вирусных сигнатур, а также для восстановления исходного состояния зараженных объектов.

АПО должно быть установлено, настроено и активировано на всех программно-технических средствах.

Все возможные каналы поступления вредоносного программного обеспечения в информационно-технологическую инфраструктуру должны быть определены, проанализированы и защищены средствами антивирусной защиты.

Контролю на предмет обнаружения вредоносных программ должна подвергаться вся информация, создаваема и обрабатываемая программно-техническими средствами, а также принимаемая (передаваемая) посредством сменных носителей информации и средств телекоммуникаций.

Любые информационные системы, используемые в локальных вычислительных сетях (далее - ЛВС) Администрации Киндальского сельского поселения (далее – Администрация), в ходе эксплуатации должны подвергаться непрерывному антивирусному мониторингу и сканированию. К таковым системам относятся сервера, рабочие станции ЛВС Администрации, а также мобильные автоматизированные рабочие места работников Администрации.

С целью эффективной борьбы с новыми видами зловредного программного обеспечения администрирование должно выполняться регулярное централизованное обновление всех средств антивирусной защиты, используемых для защиты информационных систем.

Для эффективной реализации АВЗ необходимо:

1) Унифицировать антивирусное программное обеспечение с возможностью централизованного управления;

2) Постоянное (своевременное) обновление антивирусных баз и программных компонентов.

Реализацию данного положения Антивирусной политики (далее – Политика) осуществляет ведущий специалист Администрации Киндальского сельского поселения.

II. Область действия

К области применения требований Политики относятся:

1) ЛВС Администрации;

2) Переносные автоматизированные рабочие места работников Администрации,имеющие доступ и возможность подключения в состав ЛВС;

3) Отдельные автономные автоматизированные рабочие места, не имеющие физического подключения к ЛВС,

4) Съемные носители информации.

III.Требования к подсистеме антивирусной защиты

Подсистема антивирусной защиты ЛВС предназначена для решения следующих задач:

- Перекрытие всех возможных каналов распространения вирусов, к числу которых относятся: электронная почта, разрешенные для взаимодействия с сетью Интернет сетевые протоколы (стек протоколы TCP/IP), съемные носители информации, разделяемые папки на файловых серверах;

- Непрерывный антивирусный мониторинг и периодическое антивирусное сканирование всех серверов и рабочих станций, подключаемых к ЛВС;

- Автоматическое реагирование на «заражение» компьютерными вирусами и на вирусные эпидемии, включающее в себя: оповещения, «лечение» вирусов, удаление троянских программ и очистку системы, подвергнувшейся заражению.

Подсистема антивирусной защиты ЛВС строится из следующих компонентов:

1) Средства управления, включающие в себя управляющую консоль, серверные компоненты системы антивирусной защиты, средства протоколирования и генерации отчетов;

2) Средства антивирусной защиты серверов ЛВС;

3) Средства антивирусной защиты рабочих станций;

4) Средства антивирусной защиты почтовой системы (внутренних почтовых серверов и SMTP-шлюзов на внешнем периметре сети);

5) Антивирусный шлюз, осуществляющий антивирусный контроль стек протоколов TCP/IP трафика;

6) Средства антивирусной защиты съемных носителей информации.

Категорически запрещается удалять или отключать установленные средства антивирусной защиты.

III. Ответственность

Все работники Администрации Киндальского сельского поселения, имеющие по роду своей деятельности доступ к информационным системам, несут ответственность за ущерб, причиненный вследствие нарушения настоящей Политики, в соответствии с действующим законодательством.

# 

# 