Администрация Тутаевского муниципального района

ПОСТАНОВЛЕНИЕ

от 15.01.2021 №12-п
г. Тутаев

О закреплении ответственного за антивирусную защиту и утверждении Регламента антивирусной защиты

Администрация Тутаевского муниципального района

ПОСТАНОВЛЯЕТ:

1. Назначить ответственным лицом за обеспечение комплекса мер по антивирусной защите программного обеспечения Администрации Тутаевского муниципального района и ее структурных подразделений консультанта Управления информатизации и связи Администрации Тутаевского муниципального района Наумову Елену Николаевну
2. Утвердить Регламент антивирусной защиты программного обеспечения Администрации Тутаевского муниципального района и ее структурных подразделений согласно приложению.
3. Контроль за исполнением настоящего постановления возложить на начальника управления информатизации и связи Савичева Ивана Александровича.
4. Настоящее постановление вступает в силу после его официального опубликования

Глава Тутаевского
муниципального района Д.Р. Юнусов

Приложение к постановлению
Администрации ТМР
от 15.01.2021 №12-п

Регламент антивирусной защиты программного обеспечения Администрации Тутаевского муниципального района и ее структурных подразделений

1. Общие положения

1.1. Настоящий регламент определяет требования к организации защиты Администрации Тутаевского муниципального района от воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих Администрацию Тутаевского муниципального района, за их выполнение.

1.2. Целью мероприятий по антивирусной защите является предотвращение потерь информации в Администрации Тутаевского муниципального района.

1.3. Задачами антивирусной защиты являются:

- проведение профилактических работ с применением антивирусных диагностических средств;
- непрерывное обеспечение защиты информации от действия вредоносных программ на всех этапах эксплуатации информационных систем

1.4. Объекты подлежащие защите от вирусов различными способами:

- серверы;
- рабочие станции пользователей.

2. Организация мероприятий по антивирусной защите

2.1. Консультант управления информатизации и связи Администрации Тутаевского муниципального района обеспечивает организацию работ по антивирусной защите.

2.2. В Администрации Тутаевского муниципального района планированием и проведением мероприятий по антивирусной защите занимаются выделенные для выполнения таких работ сотрудники Управления информатизации и связи Администрации Тутаевского муниципального района.

2.3. К использованию в Администрации Тутаевского муниципального района допускаются только лицензионные антивирусные средства.

2.4. Установка средств антивирусной защиты на компьютерах в Администрации Тутаевского муниципального района осуществляется уполномоченными сотрудниками Управления информатизации и связи Администрации Тутаевского муниципального района. Настройка параметров средств антивирусной защиты осуществляется сотрудниками Управления информатизации и связи Администрации Тутаевского муниципального района в соответствии руководствами по применению конкретных антивирусных средств.

2.5. Обновление антивирусных баз должно производиться не реже 1 раза в сутки автоматически, согласно возможностям программного обеспечения. В случае сбоя автоматического обновления обновление баз производится вручную с той же периодичностью.

2.6. Мероприятия по антивирусной защите на компьютерах в Администрации Тутаевского муниципального района включают в себя:

- профилактика вирусов;
- анализ ситуаций;
- применение средств антивирусной защиты;
- проведение расследований инцидентов связанных с вирусами.
- ознакомление пользователей информационных систем Администрации Тутаевского муниципального района с инструкцией пользователя по антивирусной защите (приложение 1 к регламенту)

3. Профилактика вирусов

3.1. Регулярно проводимые профилактические работы по выявлению вирусов могут полностью исключить появление и распространение вирусов в компьютере. К основным профилактическим работам и мероприятиям относятся:

- ежедневная автоматическая проверка наличия вирусов при включении компьютера;
- регулярная (не реже одного раза в квартал) выборочная проверка компьютеров на наличие вирусов, даже при отсутствии внешних проявлений вирусов;
- изучение информации по сообщениям в компьютерных журналах, газетах и Интернете о новых вирусах;
- проверка наличия вирусов на компьютере, вернувшихся с ремонта (в том числе гарантийного) в сторонних организациях;
- создание резервной копии программного продукта сразу же после приобретения;
- тщательная проверка всех поступающих и купленных программ и баз данных;
- ограничение доступа к компьютеру посторонних лиц.

3.2. Регулярную выборочную проверку наличия вирусов выполняет сотрудник Управления информатизации и связи Администрации Тутаевского муниципального района.

3.3. При обнаружении вирусов на компьютере, работающем в локальной сети, проверке подлежат все компьютеры, включенные в эту сеть и работающие с общими данными и программным обеспечением.

3.4. Создание резервной копии программного продукта выполняет сотрудник Управления информатизации и связи Администрации Тутаевского муниципального района, ответственный за внедрение этого программного продукта.

4. Анализ ситуаций

4.1. Если антивирусные программы выдают на экран дисплея сообщения о подозрении на наличие вирусов на компьютере, то прежде всего необходимо убедиться в

действительном наличии вирусов. Возможны ситуации, при которых эти сообщения являются следствием неисправности компьютера.

При возникновении подобной ситуации пользователю информационной системы необходимо приостановить работу и немедленно известить об этом руководителя подразделения, ответственного за информационную безопасность в подразделении, сотрудников Управления информатизации и связи Администрации Тутаевского муниципального района, а также смежные подразделения, использующие эти файлы в работе.

4.2. Анализ ситуации наличия вирусов или неисправности какого-либо устройства компьютера выполняет сотрудник Управления информатизации и связи Администрации Тутаевского муниципального района совместно с ответственным за информационную безопасность в подразделении. При анализе могут использоваться специальные программы проверки исправности компьютера. В результате анализа делается вывод либо об уничтожении вирусов, либо о необходимости дальнейшего восстановления работоспособности компьютера.

4.3. Основные источники вирусов:

- съемный носитель (флеш-карта, CD-ROM, DVD-ROM, мобильное дисковое устройство) на котором находятся зараженные вирусом файлы;
- компьютерная сеть, в том числе система электронной почты и Интернет;
- жесткий диск, на который попал вирус в результате работы с зараженными программами.

Если вирус проник на компьютер со съемного носителя, то необходимо определить источник и, если источник информации на съемном носителе находится в Администрации Тутаевского муниципального района, то необходимо проверить на наличие вирусов компьютер - источник информации на съемном носителе.

4.4. В случае действительного наличия вирусов привлекаются специалисты Управления информатизации и связи Администрации Тутаевского муниципального района для проведения служебного расследования.

5. Применение средств антивирусной защиты

5.1. Уничтожение вирусов выполняется сотрудником Управления информатизации и связи Администрации Тутаевского муниципального района.

5.2. Если вирус поразил какие-либо программы, то уничтожение вируса выполняется путем уничтожения программы на диске. После уничтожения зараженной программы необходимо восстановить программу, используя резервную копию программы.

5.3. Если вирус поразил файлы, то вирус уничтожается либо путем стирания этих файлов, либо путем использования специальных лечащих программ. Использование лечащих программ не дает полной гарантии восстановления файла. Поэтому после лечения необходима проверка восстановления данного файла. Лечащие программы используются лишь в тех случаях, когда отсутствует резервная копия зараженной программы либо файла с данными, либо восстановление уничтоженного файла с помощью резервной копии очень трудоемко.

5.4. В любом случае после уничтожения вирусов и восстановления зараженных программ и файлов с данными необходимо еще раз выполнить проверку наличия

вирусов, используя антивирусные программы. Перед повторной проверкой необходимо перезагрузить компьютер через выключение и последующее включение компьютера. Если повторная проверка не выявила вирусов, то можно быть уверенным в отсутствии вирусов.

5.5. Использование специализированного программного обеспечения для восстановления системных областей (FAT, загрузочной записи, и т.п.) возможно лишь в тех случаях, когда отсутствует резервная копия диска компьютера, либо его восстановление с помощью резервной копии очень трудоемко.

6. Ответственность

6.1. Ответственность за выполнение мероприятий по антивирусной защите информации на средствах вычислительной техники, эксплуатируемых подчиненными лицами в подразделении, в соответствии с требованиями настоящего Регламента, возлагается на руководителя подразделения.

6.2. Ответственность за выполнение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящего Регламента возлагается на ответственного за обеспечение информационной безопасности в подразделении и всех сотрудников подразделения.

6.3. Ответственность за проведение профилактических мероприятий по обеспечению антивирусной защиты в Администрации Тутаевского муниципального района, а также уничтожение выявленных вирусов возлагается на сотрудников Управления информатизации и связи Администрации Тутаевского муниципального района.

6.4. Периодический контроль за состоянием антивирусной защиты в Администрации Тутаевского муниципального района, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящего Регламента сотрудниками подразделений Администрации Тутаевского муниципального района осуществляется Управлением информатизации и связи Администрации Тутаевского муниципального района.

Приложение 1 к Регламенту

Инструкция пользователя по антивирусной защите Администрации Тутаевского муниципального района

В регламенте инструкция не упоминается

Общие положения

Настоящая Инструкция определяет требования к организации защиты Администрации Тутаевского муниципального района от воздействия компьютерных вирусов, устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих Администрацию Тутаевского муниципального района, за их выполнение.

Установка средств антивирусной защиты на компьютерах и настройка их параметров в Администрации Тутаевского муниципального района осуществляется уполномоченными сотрудниками Управления информатизации и связи Администрации Тутаевского муниципального района.

Обновление антивирусных баз должно производиться не реже 1 раза в сутки автоматически, согласно возможностям программного обеспечения. В случае сбоя автоматического обновления обновление баз производится вручную с той же периодичностью.

Характерные проявления вирусов

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.

Анализ ситуаций

Если антивирусные программы выдают на экран дисплея сообщения о подозрении на наличие вирусов на компьютере, то прежде всего необходимо убедиться в действительном наличии вирусов.

При возникновении подобной ситуации необходимо приостановить работу и немедленно известить об этом руководителя подразделения, ответственного за информационную безопасность в подразделении, сотрудников Управления информатизации и связи Администрации Тутаевского муниципального района, а также смежные подразделения, использующие общие программы и файлы в работе.

Анализ ситуации наличия вирусов или неисправности какого-либо устройства компьютера выполняет сотрудник Управления информатизации и связи Администрации Тутаевского муниципального района совместно ответственным за информационную безопасность в подразделении.

Основные источники вирусов:

- съемный носитель (флеш-карта, CD-ROM, DVD-ROM, мобильное дисковое устройство) на котором находятся зараженные вирусом файлы;
- компьютерная сеть, в том числе система электронной почты и Интернет;
- жесткий диск, на который попал вирус в результате работы с зараженными программами.

Если вирус проник на компьютер со съемного носителя, то необходимо определить источник и, если источник информации на съемном носителе находится в Администрации Тутаевского муниципального района, то необходимо проверить на наличие вирусов компьютер - источник информации на съемном носителе. Если источник съемного носителя - коммерческая или другая организация, то необходимо сообщить в эту организацию о факте выявления вирусов и в дальнейшем обратить особое внимание на носители информации, поступающие из этой организации.

В случае действительного наличия вирусов привлекаются Управления информатизации и связи Администрации Тутаевского муниципального района для проведения служебного расследования.

Применение средств антивирусной защиты

Уничтожение вирусов выполняется сотрудником Управления информатизации и связи Администрации Тутаевского муниципального района.

Если вирус поразил какие-либо программы, то уничтожение вируса выполняется путем уничтожения программы на диске. После уничтожения зараженной программы необходимо восстановить программу, используя резервную копию программы.

Если вирус поразил файлы, то вирус уничтожается либо путем стирания этих файлов, либо путем использования специальных лечащих программ. Использование лечащих программ не дает полной гарантии восстановления файла. Поэтому после лечения необходима проверка восстановления данного файла. Лечащие программы используются лишь в тех случаях, когда отсутствует резервная копия зараженной программы либо файла с данными, либо восстановление уничтоженного файла с помощью резервной копии очень трудоемко.

В любом случае после уничтожения вирусов и восстановления зараженных программ и файлов с данными необходимо еще раз выполнить проверку наличия вирусов, используя антивирусные программы. Перед повторной проверкой необходимо перезагрузить

компьютер через выключение и последующее включение компьютера. Если повторная проверка не выявила вирусов, то можно быть уверенным в отсутствии вирусов.

Использование специализированного программного обеспечения для восстановления системных областей (FAT, загрузочной записи, и т.п.) возможно лишь в тех случаях, когда отсутствует резервная копия диска компьютера, либо его восстановление с помощью резервной копии очень трудоемко.

Требования к сотрудникам

- Сотрудник обязан проводить антивирусный контроль всех внешних носителей информации (компакт-дисков, магнитооптических дисков и т.п.), поступающих со стороны (из внешних организаций, других подразделений Администрации Тутаевского муниципального района и т.п.) или полученных по компьютерным сетям (скопированных на общедоступный ресурс локального компьютера другими пользователями). Если антивирусная программа не работает в фоновом режиме, самому проводить проверку всех этих файлов или обращаться для этого в Управление информатизации и связи Администрации Тутаевского муниципального района;
- Во всех случаях возможного проявления действия вирусов, обнаружения файлов, пораженных вирусом или подозрении на наличие вируса сотрудник должен:
    - без попытки какого-либо лечения незамедлительно сообщить об этом любому сотруднику Управления информатизации и связи Администрации Тутаевского муниципального района и оценить с ним возможные пути заражения и распространения данного вируса;
    - совместно с сотрудником Управления информатизации и связи Администрации Тутаевского муниципального района провести лечебно-восстановительные мероприятия.
- Сотрудник обязан делать резервные копии файлов, содержащих ценную служебную информацию, если эти файлы не размещены в сетевых папках на серверах Администрации Тутаевского муниципального района;
- Сотрудник не должен самостоятельно устанавливать программное обеспечение, если это не входит в его обязанности. Запрещается устанавливать и запускать нелицензионное или не относящееся к выполнению им своих должностных обязанностей программное обеспечение;
- КАТЕГОРИЧЕСКИ ЗАПРЕЩЕНО использование съёмных носителей, принадлежащих лицам, временно допущенным к работе на компьютере в Администрации Тутаевского муниципального района (студенты-практиканты, временно замещающие, сотрудники сторонних организаций и т.п.).