ГОСУДАРСТВЕННАЯ
ЖИЛИЩНАЯ ИНСПЕКЦИЯ
РЕСПУБЛИКИ ТАТАРСТАН
ул. Б.Красная, д.15/9, г.Казань, 420111

ТАТАРСТАН
РЕСПУБЛИКАСЫНЫҢ ДӘҮЛӘТ
ТОРАК ИНСПЕКЦИЯСЕ
Б.Красная ур., д.15/9, Казан шәһәре, 420111

тел/факс. 236-91-44. E-mail: tatgi@tatar.ru, сайт: www.gji.tatarstan.ru

№ 309

ПРИКАЗ **БОЕРЫК**

«16» 08 2019 г.

Об утверждении инструкции по организации антивирусной защиты на персональных электронно-вычислительных машинах/сервере в Государственной жилищной инспекции Республики Татарстан

В соответствии с Федеральным законом от 27 июля 2006 г. № 152 ФЗ «О персональных данных» и постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, п р и к а з ы в а ю:

1. Утвердить:

инструкцию по организации антивирусной защиты на персональных электронно-вычислительных машинах/сервере в Государственной жилищной инспекции Республики Татарстан (далее - Инструкцию);

журнал проведения проверок на наличие компьютерных вирусов на персональных электронно-вычислительных машинах/сервере в Государственной жилищной инспекции Республики Татарстан (приложение № 1).

2. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник С.А. Крайнов

УТВЕРЖДЕНО
приказом начальника
Государственной
жилищной инспекции
Республики Татарстан
С.А. Крайнова

«16» 08 2019 г. № 309

Инструкция
по организации антивирусной защиты
на персональных электронно-вычислительных машинах/сервере
в Государственной жилищной инспекции Республики Татарстан

1. Общие положения

1.1 Инструкция по организации антивирусной защиты на персональных электронно-вычислительных машинах/сервере Государственной жилищной инспекции Республики Татарстан (далее - Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Доктриной информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации от 09.09.2000 г. №Пр-1895.

1.2 Настоящая Инструкция предназначена для организации порядка проведения антивирусного контроля в локальной сети передачи данных Инспекции (далее – ЛСПД) с целью предотвращения несанкционированных вредоносных воздействий на информационные ресурсы и персональные данные Инспекции и возникновения фактов заражения программного обеспечения (далее - ПО) сетевого оборудования и автоматизированных рабочих мест исполнителей компьютерными вирусами.

1.3 В настоящей Инструкции использованы следующие термины и определения:

Антивирусное ПО – набор программ для обнаружения компьютерных вирусов и других вредоносных программ и лечения инфицированных файлов, а также для профилактики – предотвращения заражения файлов или операционной системы вредоносным кодом.

Антивирусные базы – файлы, используемые антивирусным ПО при поиске вредоносных программ, периодически обновляемые разработчиком антивирусного ПО.

Антивирусный контроль – проверка информации (файла, сообщения и т.п.) на предмет наличия вредоносных программ.

Вредоносная программа – компьютерная программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информационные ресурсы.

Защищаемый компьютер – электронно-вычислительная машина (персональный компьютер или сервер), используемая для обработки данных.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Пользователь – сотрудник Инспекции или другое лицо, использующее в работе средства электронно-вычислительной техники Инспекции, назначенный приказом начальника Инспекции.

Съемный носитель информации – носитель информации, предназначенный для ее автономного хранения и независимого от места записи использования (отторгаемые жесткие магнитные диски, флэш-память, CD, DVD, дискеты и др.).

Участник ЛСПД – Инспекция, или иная организация (учреждение, предприятие), имеющее подключение к ресурсам локальной сети передачи данных Инспекции в соответствии со своими правами и полномочиями.

1.4 Требования настоящей Инструкции обязательны для выполнения всеми сотрудниками Инспекции, ведущими обработку конфиденциальной информации, персональных данных и другой информации с применением средств вычислительной техники.

1.5 Общее и методическое руководство обеспечением антивирусной защиты информационных систем и информационных систем персональных данных в ЛСПД осуществляется сектором информации (далее – СИ).

В Инспекции руководство антивирусной защитой осуществляют должностные лица, ответственные за обеспечение безопасности информации, определенные приказом начальника Инспекции.

1.6 Пользователь отвечает за обеспечение устойчивой работоспособности и информационной безопасности вверенного ему объекта вычислительной техники при работе в информационных системах и при обработке персональных данных.

1.7 Техническое обслуживание средств вычислительной техники, уборка помещения и т.п. проводятся под контролем пользователя, либо другого штатного сотрудника Инспекции.

2. Установка антивирусного ПО

2.1 Установку антивирусного ПО производят сотрудники сектора информатизации Инспекции, отвечающие за работу информационных систем и вычислительной техники, а во время их отсутствия – сотрудники, обладающие соответствующими знаниями и навыками.

2.2 В Инспекции должно использоваться только лицензионное антивирусное ПО.

2.3 Установка антивирусного ПО производится индивидуально на каждый защищаемый компьютер с обязательным предохранением настроек от изменения паролем.

2.4 Пользователям запрещается отключать средства антивирусной защиты и самостоятельно вносить изменения в настройки антивирусного ПО.

2.5 В случае необходимости использования антивирусных средств, не вошедших в перечень рекомендованных, их применение необходимо согласовать с сектором информатизации Инспекции.

3. Порядок обновления антивирусных баз

3.1 Актуализация антивирусных баз на защищаемых компьютерах, подключенных к локальной сети Инспекции, должна осуществляться ежедневно в автоматическом режиме с сервера управления антивирусной защитой локальной сети передачи Инспекции или с сервера обновлений ЗАО «Лаборатория Касперского через единую защищенную точку доступа в сеть «Интернет» (по рабочим дням).

3.2 Обновление антивирусных баз на защищаемых компьютерах, не подключенных к локальной сети Инспекции, должно осуществляться с использованием учтенных съемных носителей информации, в обязательном порядке проверяемых антивирусным ПО перед их использованием или принудительным подключением к локальной сети Инспекции.

3.3 Проверка критических областей защищаемых компьютеров, заражение которых вредоносными программами может привести к серьезным последствиям, должна проводиться автоматически при каждой его загрузке.

3.4 Актуализация антивирусных баз на защищаемых компьютерах, подключенных к локальной сети Инспекции, контролируется пользователем самостоятельно ежедневно и в случае нарушения пользователь должен не принимать никаких мер и срочно сообщить в сектор информации Инспекции, который в свою очередь должен официально сообщить о данном инциденте информационной безопасности в Центр информационных технологий Республики Татарстан (далее – ЦИТ РТ).

4. Требования к проведению антивирусного контроля

4.1 Пользователь осуществляет контроль за целевым использованием автоматизированного рабочего места, а также всех его внешних устройств.

4.2 Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, файлы данных, сообщения электронной почты и т.д.), получаемая и передаваемая по телекоммуникационным каналам, а также данные на съемных носителях информации. Контроль входящей и исходящей информации на защищаемых компьютерах должен осуществляться непрерывно посредством постоянно работающего компонента антивирусного ПО («монитора»).

4.3 Все программное обеспечение, устанавливаемое на защищаемые компьютеры, должно предварительно проверяться на наличие вредоносных программ.

4.4 Полная проверка сетевых ресурсов и рабочих станций на наличие компьютерных вирусов производится не реже одного раза в месяц в обязательном порядке с записью в «Журнал проведения проверок на наличие компьютерных вирусов на ПЭВМ/сервере в Государственной жилищной инспекции Республики Татарстан».

4.5 Внеочередной антивирусный контроль всех дисков и файлов защищаемого компьютера должен выполняться:

– сразу после установки или изменения ПО;

– после подключения автономного компьютера к локальной сети;

– при возникновении подозрения на наличие вредоносных программ (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках, сбоях и т.п.).

4.6 В сомнительных случаях для определения факта наличия или отсутствия вредоносных программ к проверке необходимо привлечь специалистов ЦИТ РТ.

Администратор безопасности информации Инспекции обязан регулярно докладывать заведующему сектора информации Инспекции о результатах периодической проверки состояния антивирусной защиты.

5. Действия пользователей при обнаружении вредоносных программ

5.1 В случае обнаружения при проведении антивирусной проверки вредоносных программ пользователи обязаны:

– приостановить все операции, связанные с обработкой файлов на защищаемом компьютере;

– немедленно поставить в известность о факте обнаружения вредоносных программ сектор информации Инспекции, владельцев зараженных или поврежденных вредоносными программами файлов, а также смежные подразделения, использующие эти файлы в работе;

- сделать запись в «Журнал проведения проверок на наличие компьютерных вирусов на ПЭВМ/сервере в Государственной жилищной инспекции Республики Татарстан»;

– совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

– после доклада в ЦИТ РТ, по разрешению заведующего сектора информатизации, провести лечение зараженных файлов (при необходимости привлечь специалистов ЦИТ РТ);

– в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на отторгаемом носителе в ЦИТ РТ для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;

- по факту обнаружения зараженных вирусом файлов составить служебную записку в ЦИТ РТ, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

6. Ответственность за выполнение требований Инструкции

6.1 Ответственность за организацию антивирусной защиты информации на компьютерах, эксплуатируемых пользователями, и их ознакомление с Инструкцией несет администратор информационной безопасности Инспекции.

6.2 Ответственность за соблюдение требований Инструкции на своих рабочих местах несут пользователи.

6.3 Ответственность за своевременное обновление антивирусных баз и получение новых лицензионных ключей при истечении их срока действия несет администратор информационной безопасности Инспекции.

6.4 За нарушение требований Инструкции пользователи несут дисциплинарную ответственность в соответствии с действующим законодательством.

Приложение №1

УТВЕРЖДЕНО
приказом начальника
Государственной
жилищной инспекции
Республики Татарстан

С.А. Крайнов
«16» 08 2019 г. № 309

ЖУРНАЛ
проведения проверок на наличие компьютерных вирусов на ПЭВМ/сервере
в Государственной жилищной инспекции Республики Татарстан

№ п/п	Дата проверки	ФИО сотрудника, проводившего проверку	Инв. № ПЭВМ/сервера	ФИО сотрудника, работающего на проверяемом ПЭВМ	Программные средства, с помощью которых проведена проверка	Результат проверки	Примечание (принятые меры)

ЛИСТ ОЗНАКОМЛЕНИЯ

с Приказом ГЖИ РТ от 16.07.19 № 309

«Об утверждении инструкции по организации антивирусной защиты на персональных электронно-вычислительных машинах/сервере в Государственной жилищной инспекции Республики Татарстан»

_____

(наименование структурного подразделения)

№ п/п	Ф.И.О сотрудника	Подпись	Дата ознакомления