МЭРИЯ ГОРОДСКОГО ОКРУГА ТОЛЬЯТТИ

РАСПОРЯЖЕНИЕ

13.01.2017 № 102-р/1

г. Тольятти, Самарской области

Об утверждении инструкции
по организации антивирусной защиты
информационных систем
в мэрии городского округа Тольятти.

В целях реализации Федерального закона от 27.07.2006 г. № 152-ФЗ "О персональных данных", в соответствии с Постановлением Правительства Российской Федерации от 21.03.2012 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", руководствуясь Уставом городского округа Тольятти,

1. Утвердить прилагаемую инструкцию по организации антивирусной защиты информационных систем в мэрии городского округа Тольятти.

2. Руководителю департамента информационных технологий и связи мэрии городского округа Тольятти Балашовой Е.В. разместить настоящее распоряжение на официальном портале мэрии городского округа Тольятти.

3. Руководителям органов мэрии городского округа Тольятти не позднее десяти дней с момента принятия настоящего распоряжения ознакомить персонал с настоящим распоряжением.

4. Контроль за исполнением настоящего распоряжения оставляю за собой.

Мэр С.И.Андреев

УТВЕРЖДЕНА
распоряжением мэрии
городского округа Тольятти
от 13.01. 2016г. № 102-р/1

ИНСТРУКЦИЯ

по организации антивирусной защиты информационных систем в мэрии городского округа Тольятти

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет требования к организации антивирусной защиты информационных систем и информационных ресурсов мэрии городского округа Тольятти (далее – мэрии).

1.2. Действие настоящей Инструкции распространяется на структурные подразделения органов мэрии.

1.3. Вредоносная программа – программа (в том числе компьютерный вирус), предназначенная для осуществления несанкционированного доступа или иного воздействия на ресурсы информационных систем.

Вредоносная программа способна выполнять ряд функций, в том числе:

- скрывать признаки своего присутствия в программной среде рабочей станции (сервера);
- обладать способностью к самодублированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать произвольным образом) код программ в оперативной памяти;
- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
- искажать произвольным образом, блокировать и/или подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

1.4. Администратор системы антивирусной защиты (далее - Администратор) – сотрудник отдела информационной безопасности департамента информационных технологий и связи мэрии (далее - ОИБ ДИТиС), назначаемый приказом руководителя ДИТиС.

1.5. В целях обеспечения защиты от деструктивных воздействий компьютерных вредоносных программ производится непрерывный антивирусный контроль. Обязательному антивирусному контролю подлежит любая информация, поступающая на средства вычислительной техники, в том числе получаемая от сторонних организаций.

1.6. Основными задачами системы обеспечения антивирусной защиты являются:

- исключение или существенное затруднение противоправных действий в отношении информационных систем мэрии, как носителей защищаемой информации;
- обеспечение условий для устойчивой бесперебойной работы информационных систем, сетей передачи данных.

1.7. Объектом защиты от воздействия вредоносных программ являются серверы, автоматизированные рабочие места (далее - АРМ) сотрудников и каналы передачи информации мэрии.

1.8. Обеспечение антивирусной защиты включает:

- регулярные профилактические работы;
- анализ ситуации проявления вредоносных программ и причины их появления;
- уничтожение вредоносных программ на АРМ и серверах мэрии;
- принятие мер по предотвращению причин появления вредоносных программ.

1.9. Для выполнения требований по антивирусной защите АРМ и серверов мэрии используется специализированное программное обеспечение (далее - ПО), обеспечивающее постоянную автоматическую антивирусную защиту и контроль чистоты информационных массивов данных от вредоносных программ.

1.10. Организация работ по антивирусной защите и ответственность за сопровождение системы антивирусной защиты возлагается на ОИБ ДИТиС.

1.11. Ответственность за контроль установленного порядка антивирусной защиты возлагается на администратора.

1.12. Все программные модули и задачи системы антивирусной защиты функционируют в автоматическом режиме без участия пользователей и без помех для работы системного и прикладного ПО.

1.13. Процесс плановой полной проверки файловой системы АРМ пользователей и серверов мэрии проводится во время наименьшей нагрузки оборудования пользовательскими задачами.

1.14. Для пользователей АРМ запрещена возможность изменения настроек и параметров защиты антивирусных средств на своей рабочей станции, эти действия производит администратор с помощью средств централизованного управления или вручную.

1.15. По факту появления и воздействия вредоносных программ, повлекших неустойчивую работу и (или) выход из строя технологического оборудования, сети передачи данных и информационных массивов мэрии, проводится разбор инцидента информационной безопасности.

2. ТРЕБОВАНИЯ К АНТИВИРУСНОМУ ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

2.1. Использование только лицензионного антивирусного ПО, сертифицированного в соответствии с требованиями ФСТЭК РФ для защиты информации ограниченного доступа.

2.2. Обнаружение возможно большего числа известных вредоносных программ, в том числе вирусов, деструктивного кода (макро-вирусы, объектов ActiveX, апплетов языка Java и т.п.), а также максимальная готовность быстрого реагирования на появление новых видов вирусных угроз.

2.3. Исчерпывающий список защищаемых точек (почтовые, файловые серверы, АРМ и т.д.) возможного проникновения вредоносных программ.

2.4. Обеспечение обновлений, консультаций и других форм сопровождения эксплуатации поставщиком антивирусного ПО.

2.5. Возможность автоматического распространения обновлений антивирусных баз на каждую рабочую станцию мэрии.

2.6. Соответствие системных требований антивирусного ПО платформам, характеристикам и комплектации применяемой вычислительной техники.

2.7. Надежность и работоспособность антивирусного ПО в любом из предусмотренных режимов работы, в программной среде с русскоязычным интерфейсом.

2.8. Наличие документации, необходимой для практического применения и освоения антивирусного ПО, на русском языке.

3. ДЕЙСТВИЯ АДМИНИСТРАТОРА ПО ШТАТНОМУ УПРАВЛЕНИЮ СРЕДСТВАМИ АНТИВИРУСНОГО КОНТРОЛЯ

3.1. В штатном режиме работы антивирусной системы администратор выполняет:

- установку средств антивирусной защиты на все объекты антивирусной защиты в порядке, описанном в эксплуатационной документации;
- контроль наличия связи между сервером администрирования и защищаемыми объектами;
- необходимые обновления версий средств антивирусной защиты на объектах антивирусной защиты;
- контроль над выполнением задач постоянной защиты;
- настройку автоматических проверок объектов антивирусной защиты не реже одного раза в неделю с целью профилактики;
- контроль актуальности версий антивирусных баз и модулей сканирования ПО сервера администрирования;
- обработку сведений, поступающих от средств антивирусной защиты;
- формирование сводных отчетов о работе средств антивирусной защиты, инцидентах и проч.;
- обработку отчетов о состоянии логических сетей;
- формирование отчетов о работе средств антивирусной защиты логической сети.

3.2. Процесс управления системой антивирусной защиты включает в себя следующие действия администратора:

- внесение изменений в политику антивирусной защиты;
- управление средствами антивирусной защиты, входящими в состав системы антивирусной защиты;
- мониторинг событий, информация о которых поступает от средств антивирусной защиты с объектов защиты.

3.3. В обязанности администратора входит периодическое проведение мероприятий, обеспечивающих возможность анализа результатов работы системы антивирусной защиты:

- разработка отчетов о работе средств антивирусной защиты;
- разработка сводных отчетов о работе средств антивирусной защиты, инцидентах и пр.

В отчетах о состоянии системы антивирусной защиты отражается следующая информация:

- количество обнаруженных вредоносных программ за данный период;
- объекты, где наблюдается наибольшая частота обнаружения вредоносных программ;
- список зараженных объектов.

4. ДЕЙСТВИЯ АДМИНИСТРАТОРА ПО НЕШТАТНОМУ УПРАВЛЕНИЮ СРЕДСТВАМИ АНТИВИРУСНОГО КОНТРОЛЯ

4.1. В случае заражения АРМ, серверов вредоносными программами администратор выполняет следующие действия:

- оперативно принимает меры по предотвращению распространения заражения вредоносными программами и при необходимости отключает от сети зараженную рабочую станцию, сервер;
- централизованно обновляет антивирусные базы сервера администрирования и всех объектов антивирусной защиты;
- проверяет состояние всех объектов антивирусной защиты, наличие зараженных рабочих станций в случае обнаружения пораженных узлов;
- проводит действия, направленные на устранение вредоносной программы на всех пораженных информационных системах мэрии;
- по завершении мероприятий по устранению последствий заражения восстанавливает работоспособность рабочей станции и передает ее ответственному пользователю.

5. ДЕЙСТВИЯ АДМИНИСТРАТОРА ПО УНИЧТОЖЕНИЮ ВРЕДОНОСНЫХ ПРОГРАММ

5.1. Нейтрализация действия вредоносной программы при нарушении функционирования информационной системы осуществляется путем уничтожения вредоносной программы на жестком диске либо на ином электронном носителе.

5.2. Нейтрализация действия вредоносной программы при поражении файлов осуществляется либо путем стирания этих файлов, либо путем использования специального "лечащего" режима антивирусного ПО. В случае применения "лечащего" режима производится последующая проверка целостности информации пораженного файла. "Лечащий" режим используется только при отсутствии резервной копии файла.

5.3. После уничтожения вредоносных программ и восстановления файлов выполняется повторная проверка наличия вредоносных программ. Перед повторной проверкой производится перезагрузка сервера или рабочей станции через выключение и последующее включение.

6. ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ МЭРИИ ПРИ ОБНАРУЖЕНИИ ВРЕДОНОСНОЙ ПРОГРАММЫ

6.1. При возникновении подозрения на наличие вредоносной программы, компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, исчезновение файлов, частое появление сообщений о системных ошибках и т.п.), а также в случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

приостановить работу;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов непосредственного руководителя и администратора;

сообщить администратору предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, необходимость дальнейшего использования пораженных вирусом файлов.

7. РАЗБОР ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ВЫЗВАННОГО ВРЕДОНОСНОЙ ПРОГРАММОЙ.

7.1. В процессе проведения разбирательства инцидента ИБ, вызванного вредоносной программой, устанавливаются:

- дата, время и место обнаружения вредоносной программы;
- информационные ресурсы, затронутые вредоносной программой;
- уровень критичности инцидента ИБ, вызванного вредоносной программой;
- характер и размер реального и потенциального ущерба;
- обстоятельства, способствовавшие проникновению и запуску вредоносной программы.

7.2. Осуществляющий разбирательство сотрудник ОИБ ДИТиС в процессе проведения расследования инцидента ИБ при необходимости запрашивает информацию в органах мэрии. Запрос направляется на имя руководителя

органа мэрии с указанием сроков предоставления информации (с учетом необходимости ее анализа, сбора и подготовки).

7.3. После получения необходимой информации по инциденту ИБ осуществляющий разбирательство сотрудник ОИБ ДИТиС проводит анализ полученных данных.

7.4. С целью минимизации последствий инцидента ИБ возможно временное отключение прав доступа у пользователя к информационным ресурсам (далее - ИР) на время проведения расследования.

7.5. Восстановление временно отключенных у пользователя прав доступа к ИР производится по заявке осуществляющего разбирательство сотрудника ОИБ ДИТиС.

7.6. Собранная в процессе разбирательства инцидента ИБ информация фиксируется осуществляющим разбирательство сотрудником ОИБ ДИТиС в карточке инцидента ИБ (приложение №1 к настоящей Инструкции).

7.7. Осуществляющий разбирательство сотрудник направляет акт разбирательства инцидента ИБ руководителю ДИТиС для последующей передачи руководителям органов мэрии, затронутых инцидентом ИБ.

7.8. На основании полученного акта разбирательства инцидента ИБ руководитель органа мэрии, затронутого инцидентом ИБ, в срок не более трех рабочих дней организует проведение мероприятий, направленных на снижение рисков ИБ в будущем:

- анализ и пересмотр имеющихся прав доступа к информационным ресурсам у пользователей;
- доведение до всех сотрудников органа мэрии требований правовых актов в области ИБ.

8. ОТВЕТСТВЕННОСТЬ

8.1. Организация мероприятий по централизованной антивирусной защите мэрии возлагается на администратора.

8.2. Администратор несет ответственность за формирование политики антивирусной защиты, организацию своевременной инсталляции средств антивирусной защиты информации и централизованное обновление баз

данных вирусных описаний на комплексе программно-технических средств мэрии.

8.3. Выполнение технических мероприятий по централизованной антивирусной защите в мэрии производится непосредственно администратором.

8.4. Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации и требований настоящей Инструкции несут сотрудники органов мэрии, за которыми закреплены соответствующие АРМ.

Приложение №1

к инструкции по организации антивирусной защиты информационных систем в мэрии городского округа Тольятти

Карточка инцидента информационной безопасности, вызванного вредоносной программой

Дата инцидента ИБ _____ Номер инцидента ИБ _____

Информация о сообщившем:

Ф.И.О.	должность	Подразделение органа мэрии	Рабочий телефон

Тип инцидента:	*Действительный* ☐		*Подозрение* ☐	
Предполагаемый вид вредоносной программы	*Шифровальщик* ☐	*Компьютерный вирус* ☐	*Сетевой червь* ☐	*Троянская программа* ☐
Последствия инцидента:	*без последствий* ☐	*нарушение работоспособностикомпонентов ИС* ☐	*нарушение целостности ИР, фальсификация документов* ☐	*нарушение режима конфиденциальности информации* ☐
Объект, которому нанесен ущерб:	*Информация* ☐		*Программное обеспечение* ☐	
Действия, предпринятые для разрешения инцидента:	*Описание действий*		*никаких действий не требуется* ☐	*Без привлечения внешнего исполнителя* ☐	*С привлечением внешнего исполнителя* ☐

Дополнительная информация

_____

_____

_____

_____

_____

Ф.И.О. сотрудника ОИБ ДИТиС, проводившего разбирательство

_____