ДЕПАРТАМЕНТ ЗДРАВООХРАНЕНИЯ И СОЦИАЛЬНОГО РАЗВИТИЯ ОРЛОВСКОЙ ОБЛАСТИ

КАЗЁННОЕ УЧРЕЖДЕНИЕ ОРЛОВСКОЙ ОБЛАСТИ «УПРАВЛЕНИЕ СОЦИАЛЬНОЙ ЗАЩИТЫ НАСЕЛЕНИЯ Г. ОРЛА»

27 декабря 2012 года № 62

ПРИКАЗ
об утверждении положения об антивирусной защите

В целях реализации Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21 марта 2012 года № 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», в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 1 ноября 2012 года № 1119,

ПРИКАЗЫВАЮ:

1. Утвердить положение об антивирусной защите согласно Приложению 1 к настоящему приказу.
2. Контроль за исполнением приказа возложить на ответственного за организацию обработки персональных данных по учреждению – заместителя директора Е. М. Китаеву.
3. Настоящий приказ вступает в силу с 1 января 2013 года.

Директор КУ ОО «УСЗН г. Орла» В. М. Мильшин

Приложение 1

УТВЕРЖДЕНО
Приказом директора казенного учреждения
Орловской области «Управление
социальной защиты населения г. Орла »
от 27 декабря 2012 года № 62

Директор казенного учреждения Орловской
области «Управление социальной защиты
населения г. Орла»
В. М. Мильшин

Положение об антивирусной защите

1. Термины и определения

Компьютерным вирусом называется программа, способная создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты или ресурсы компьютерных систем, сетей и так далее без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения. На сегодняшний день известно 6 основных типов вирусов: файловые, загрузочные, призраки (полиморфные), невидимки, скрипт-вирусы и макро-вирусы. Следует отличать вирусы от вредоносных кодов. К ним относятся Интернет-черви и программы, получившие название "Троянские кони".

Основные симптомы вирусного поражения: замедление работы некоторых программ, увеличение размеров файлов (особенно выполняемых), появление не существовавших ранее подозрительных файлов, уменьшение объема доступной оперативной памяти (по сравнению с обычным режимом работы), внезапно возникающие разнообразные видео и звуковые эффекты.

При всех перечисленных выше симптомах, а также при других нестандартных проявлениях в работе системы (неустойчивая работа, частые самостоятельные перезагрузки и прочее) следует немедленно произвести проверку системы на наличие вирусов.

Зараженный диск - это диск, в загрузочном секторе которого находится программа - вирус. После запуска программы, содержащей вирус, становится возможным заражение других файлов. Наиболее часто вирусом заражаются загрузочный сектор диска и исполняемые файлы, имеющие расширения EXE, COM, SYS или BAT. Крайне редко заражаются текстовые и графические файлы.

Зараженная программа - это программа, содержащая внедренную в нее программу-вирус.

2. Общие положения

2.1. Настоящее Положение определяет требования к организации защиты информации в казенном учреждении Орловской области «Управление

социальной защиты населения г. Орла» (далее – Учреждение) от воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников Учреждения, эксплуатирующих автоматизированные рабочие места, на которых ведется обработка персональных данных.

2.2. Целью мероприятий по антивирусной защите является предотвращение потерь информации в ИСПДн.

2.3. Задачами антивирусной защиты являются:

- своевременное обеспечение средствами антивирусной защиты информации автоматизированные рабочие места Учреждения.
- проведение профилактических работ на автоматизированных рабочих местах с применением антивирусных диагностических средств;
- непрерывное обеспечение защиты информации от действия вредоносных программ на всех этапах эксплуатации ИСПДн.
- проверка входящего/исходящего потоков Интернет;
- контроль входящей/исходящей почты и прикрепленных файлов;

3. Организация мероприятий по антивирусной защите

3.1. Сотрудник Учреждения, ответственный за организацию защиты персональных данных при их обработке в информационных системах персональных данных обеспечивает организацию работ по антивирусной защите.

3.2. Организации антивирусной защиты информации на объектах информатизации достигается путём:

– установки и применения средств антивирусной защиты информации;

– обновления баз данных средств антивирусной защиты информации;

– действий должностных лиц при обнаружении заражения информационно-вычислительных ресурсов программными вирусами.

3.2.1. Организация работ по антивирусной защите информации возлагается на должностных лиц, осуществляющих контроль за антивирусной защитой (администратора безопасности ИСПДн), а методическое руководство и контроль над эффективностью предусмотренных мер защиты информации на начальников ОСЗН.

3.2.2. Защита информации от воздействия программных вирусов на объектах информатизации должна осуществляться посредством применения средств антивирусной защиты. Порядок применения средств антивирусной защиты устанавливается с учетом следующих требований:

– обязательный входной контроль на отсутствие программных вирусов всех поступающих на объект информатизации носителей информации, информационных массивов, программных средств общего и специального назначения;

– периодическая проверка пользователями жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка используемых в работе носителей информации перед началом работы с ними на отсутствие программных вирусов;

– внеплановая проверка носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса;

– восстановление работоспособности программных средств и информационных массивов в случае их повреждения программными вирусами.

3.2.3. К использованию допускается только лицензированные, сертифицированные по требованиям ФСТЭК России антивирусные средства.

3.2.4. Порядок применения средств антивирусной защиты во всех случаях устанавливается с учетом следующих требований:

– входной антивирусный контроль всей поступающей на внешних носителях информации и программных средств любого назначения.

– входной антивирусный контроль всей информации поступающей с электронной почтой;

– входной антивирусный контроль всей поступающей информации из сети Internet;

– выходной антивирусный контроль всей исходящей информации на любых внешних носителях и/или передаваемой по локальной сети на другие рабочие станции/сервера, а так же передача информации посредством электронной почты;

– периодическая антивирусная проверка на отсутствие компьютерных вирусов на жестких дисках рабочих станций и серверов;

– обязательная антивирусная проверка используемых в работе внешних носителей информации;

– постоянный антивирусный контроль на рабочих станциях и серверах с использованием резидентных антивирусных мониторов в автоматическом режиме;

– обеспечение получения обновлений антивирусных программ в автоматическом режиме, включая обновления вирусных баз и непосредственно новых версий программ;

– неплановая антивирусная проверка внешних носителей и жестких дисков рабочих станций и серверов на отсутствие компьютерных вирусов в случае подозрения на наличие компьютерного вируса;

– восстановление работоспособности программных и аппаратных средств, а так же непосредственно информации в случае их повреждения компьютерными вирусами.

3.2.5.Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке и руководством по эксплуатации конкретного антивирусного программного продукта.

3.2.6. При обнаружении на носителе информации или в полученных файлах программных вирусов пользователи докладывают об этом в подразделение по защите конфиденциальной информации или ответственному сотруднику, и принимают меры по восстановлению работоспособности программных средств и данных.

О факте обнаружения программных вирусов сообщается в орган, от которых поступили зараженные файлы, для принятия мер по локализации и устранению программных вирусов.

Перед отправкой массивов информации и программных средств, осуществляется ее проверка на наличие программных вирусов.

При обнаружении программных вирусов пользователь обязан немедленно прекратить все работы на АРМ, поставить в известность администратора безопасности ИСПДн и принять меры к их локализации и удалению с помощью имеющихся антивирусных средств защиты.

При функционировании АРМ в качестве рабочей станции вычислительной сети производится ее отключение от локальной сети, локализация и удаление программных вирусов в вычислительной сети.

Ликвидация последствий воздействия программных вирусов осуществляется администратором безопасности ИСПДн.

3.2.7. Организация антивирусной защиты конфиденциальной информации должна быть направлена на предотвращение заражения рабочих станций, входящих в состав локальных компьютерных сетей, и серверов различного уровня и назначения вирусами.

3.2.8. Необходимо постоянно осуществлять обновление вирусных баз. Частоту обновления установить в зависимости от используемых антивирусных средств и частоты выпуска обновления указанных баз.

3.2.9. Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке, руководством по эксплуатации конкретного антивирусного программного продукта и инструкцией по антивирусной защите.

3.2.10. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в информационных системах возлагается на администратора безопасности ИСПДн.

3.2.11. Обновление антивирусных баз должно производиться, согласно возможностям программного обеспечения.

3.2.12. Мероприятия по антивирусной защите на компьютерах Управления включают в себя:

- профилактика вирусов;
- анализ ситуаций;
- применение средств антивирусной защиты;
- проведение расследований инцидентов связанных с вирусами.

4. Профилактика вирусов

4.1. 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;
- . тщательная проверка всех поступающих и купленных программ и баз данных;
- . ограничение доступа к компьютеру посторонних лиц.

4.2. Регулярную выборочную проверку наличия вирусов выполняет сотрудник Учреждения, за которым закреплено автоматизированное рабочее место.

4.3. 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.

4.4. Проверку всех поступающих и купленных программ выполняет Администратор информационной безопасности

5. Анализ ситуаций

5.1. 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 необходимо приостановить работу и немедленно известить об этом непосредственного руководителя и (или) администратора информационной безопасности.

5.2. При анализе ситуации наличия вирусов или неисправности какого-либо устройства компьютера могут использоваться специальные программы проверки исправности компьютера.

В результате анализа делается вывод либо об уничтожении вирусов, либо о необходимости дальнейшего восстановления работоспособности компьютера.

5.3. Основные источники вирусов:

- съемный носитель (дискета, 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.

6. Применение средств антивирусной защиты

6.1. Уничтожение вирусов выполняется пользователем автоматизированного рабочего места.

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

6.3. 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.

6.4. 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.