УДК 004:056-55

ЗАЩИТА ИНФОРМАЦИИ

Бакунькина Н.М., студентка 2 курса факультета информационных систем и технологий
Научный руководитель – Горбоконенко В.Д., доцент
ФГБОУ ВО Ульяновского государственного технического университета

Ключевые слова: *защита информации, вирусы, угроза информации, программы.*

Работа посвящена выявлению источников угроз информации и определению способов защиты от них.

С выходом в свет передовых средств вычислительной техники и телекоммуникаций классические правонарушения - кража, жульничество, шпионаж, вымогательство трансформировались в обновлённые формы. Кроме этого, были замечены опасности, связанные с внесением и включением технических перемен в способы вычислительной техники и способы связи, хищением носителей информации: дискет, описаний, распечаток [1]. Для контроля за данной ситуацией и введения ее в правовое поле разработан ряд документов.

Существует Федеральный закон N 149-ФЗ от 2006 г. «Об информации, информационных технологиях и о защите информации».

Федеральный закон регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

Особое внимание в этом законе следует обратить на понятие «информация», как на объект правовых отношений. Защита информации представляет принятие правовых, организационных и технических мер. Неправомерный доступ, уничтожение, модифицирование, копирование,

соблюдение конфиденциальности информации ограниченного доступа, недопущение воздействия на технические средства обработки информации, возможность восстановления уничтоженной информации – неполный перечень проблем, которые рассматриваются в данном законе.

Национальный стандарт ГОСТ Р 50922-2006 «Защита информации» распространяется на основные средства защиты информации и средства контроля эффективности защиты информации, входящие в состав техники защиты информации.

Настоящий стандарт устанавливает номенклатуру основных показателей качества средств защиты информации: от утечки по техническим каналам, от несанкционированного доступа, а также средств контроля эффективности защиты информации, которые должны быть включены в тактико-технические задания на научно-исследовательские и опытно-конструкторские работы по определению и реализации перспектив развития этой группы продукции, и национальные стандарты [3].

В реальное время, опасность более всего исходит от компьютерных вирусов, которые искажают или же губят актуально весомую, ценную информацию, что имеет возможность привести не только к денежным потерям, но и к человеческим жертвам.

Всеобщие способы обороны информации актуальны для защиты от вирусов, все же их мало. Нужно и использование специализированных программ для ограждения от вирусов. Эти программы можно разделить на несколько видов: детекторы, доктора, ревизоры, фильтры и иммунизаторы.

Детекторы дают возможность показывать файлы, зараженные одним из нескольких популярных вирусов. Эти программы проводят проверку, есть ли в файлах на обозначенном пользователем диске специфичная для представленного вируса комбинация байтов. При ее появлении в каком-либо файле на экран выводится сообщение.

Соответственно, что программа не опознается детекторами как зараженная, не значит, что она не больна - в ней может сидеть какой-нибудь новый вирус или немного изменённая версия давнишнего вируса, неведомые программам-детекторам.

Основная масса программ-детекторов имеет функцию "доктора", т.е. пробует возвратить зараженные файлы или области диска в их начальное

состояние. Те файлы, которые не получилось возобновить, делаются неработоспособными или, удаляются.

Многие программы-доктора могут "лечить" только лишь от некоторого фиксированного набора вирусов, в следствии этого они становятся неактуальными. Но кое-какие программы имеют все шансы обучиться не только методикам обнаружения, но и методикам исцеления от новых вирусов.

Программы-ревизоры имеют две стадии работы. В начале они запоминают сведения о состоянии программ и системных областей дисков. Ожидается, что в данный момент программы и системные области дисков не заражены. Впоследствии чего с поддержкой программы-ревизора возможно всегда сопоставить состояние программ и системных областей дисков с начальным. О обнаруженных несоответствиях информируется пользователю.

Для испытания, не поменялся ли файл, кое-какие программы-ревизоры проводят проверку длины файла. Но данное испытание недостаточно - некоторые вирусы не меняют длину зараженных файлов. Более достоверная проверка – прочитать целый файл и определить его контрольную необходимую сумму. Изменить файл так, чтобы его контрольная сумма осталась прежней, практически нельзя.

Есть ещё программы фильтры, которые размещаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые применяются вирусами для размножения и нанесения вреда, и информируют о них пользователю.

Многие программы-фильтры не "ловят" сомнительные действия, а проводят проверку вызываемых на выполнение программ на присутствие вирусов. Это грозит замедлению работы компьютера.

Впрочем, положительные качество применения программ-фильтров очень значимы – они дают возможность выявить все вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить.

Иммунизаторы модифицируют программы и диски так, что это никак не отображается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы очень неэффективны [4].

В вычислительной технике понятие защищённости считается очень широким. Оно предполгает и надежность работы компьютера, и сохранность ценных данных, и защиту информации от внесения в нее перемен неуполномоченными лицами, и сбережение тайны переписки в электронной связи. Естественно, во всех цивилизованных государствах на безопасности граждан стоят законы, но в вычислительной технике правоприменительная практика пока не развита, а законотворческий процесс не успевает за развитием технологий, и надежность работы компьютерных систем во многом опирается на меры самозащиты.

Библиографический список:

1. Ясенев В.Н. Информационная безопасность в экономических системах [Текст]: учеб. пособие для студ. экономических специальностей высших учебных заведений. / В.Н. Ясенев. – Н. Новгород: Изд. ННГУ, 2006. – 18 с.

2. О защите информации на 2006 год: ФЗ от 27.07.2006 г. N 149-ФЗ // Российская газета. – 2006. – 29 июля. – С.48

3. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.-Введ. 01-02-2008.-М.: Стандартинформ, 2008 -7 с.

4. Безруков Н.Н. Компьютерные вирусы [Текст] - М.: Наука, 1991. – с.

PROTECTION OF INFORMATION

Bakunkina N.M.

Key words: information protection, viruses, information threat, programs.

The work is devoted to identifying sources of information threats and defining ways to protect against them.