Опубликовано: Климентьев К.Е. Технические аспекты проблемы компьютерных вирусов в сфере промышленной автоматизации // В сб. «Вестник СамГТУ. Сер.: Технические науки», 2005. – С. 176-179.

УДК 681.322

К.Е. Климентьев

ТЕХНИЧЕСКИЕ АСПЕКТЫ ПРОБЛЕМЫ КОМПЬЮТЕРНЫХ ВИРУСОВ В СФЕРЕ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ

Обсуждаются технические аспекты проблемы компьютерных вирусов в SCADA-системах и операционных системах реального времени. Приводятся результаты практических исследований и предлагаются средства для создания защищенных от вирусов систем.

Под компьютерным вирусом (КВ) будем понимать программу для ЭВМ, способную к несанкционированному созданию своих функционально идентичных копий. В настоящее время КВ представляют собой острейшую проблему в вычислительных системах и сетях общего назначения. Типичной (но не единственно возможной!) жизненной средой КВ являются операционные системы фирмы Microsoft, функционирующие на аппаратных платформах IA-32 и использующие сетевые технологии на базе TCP/IP. Широкое распространение КВ объективно связано со стандартизацией и унификацией аппаратных и программных средств, методов обработки и протоколов обмена данными. В большинстве случаев сами КВ являются косвенной причиной причиняемых убытков, так как механизм их негативного воздействиях заключается в искажении и блокировании и информационных потоков, питающих нерационально устроенную систему торговых, финансовых и прочих отношений, в возбуждении социальных эффектов типа “вирусной паранойи” и пр. Редким примером непосредственного разрушающего воздействия является активация деструктивного вируса Win95.CIH 26 апреля 1999 года.

Однако существует сфера применения вычислительной техники, в которой практически любая вирусная атака способна привести к прямому ущербу, это - сфера промышленной автоматизации. Основным деструктивным фактором при этом является несанкционированное использование КВ системных ресурсов – оперативной памяти, дискового пространства, процессорного времени.

На текущий момент имеется очень мало достоверной информации о КВ в этой сфере. В начале 2003 г. сетевой червь Slammer (другое название - Sapphire) на 5 часов парализовал работу АСУ ТП атомной электростанции Davis-Besse (США). По непроверенным данным в августе того же года причиной массовых отключений в энергетических системах США и Канады стал вирус Blaster (другие названия - MSBlast, LoveSan). Основным (но не единственным!) фактором, обеспечившим возможность упомянутых вирусных инцидентов, послужила интеграция специализированных средств управления технологическим процессами с унифицированными средствами обработки и передачи информации. Тенденция к подобного рода интеграции наблюдается во всем мире в сфере промышленной автоматизации примерно с середины 90-х годов XX века. В качестве примеров проявления тенденции можно отметить:

- использование модификаций шины PCI (CompactPCI и PXI) в качестве системной шины для промышленных контроллеров;
- использование программного обеспечения общего назначения (например, MS Windows) для создания систем промышленной автоматизации;
- использование универсальных физических сред (Ethernet) и протоколов (TCP/IP) для обслуживания распределенных систем промышленной автоматизации (в частности, для решения задач удаленного управления).

В то же время **не имеется никаких достоверных данных о возможности существования вирусной угрозы в специализированных программных средах, используемых исключительно для создания систем промышленной автоматизации.** Данный доклад посвящен рассмотрению именно этой актуальной проблемы.

Проблема была рассмотрена в рамках исследований, проводимых на кафедре ИСТ Самарского государственного аэрокосмического университета силами преподавателей и студентов в процессе подготовки методического обеспечения для дисциплин “Методы и средства защиты компьютерной информации”, “Системы реального времени” и “Программные средства АСНИ” /1/.

В рассмотрение попали следующие классы системного и прикладного программного обеспечения:

- UNIX-подобные операционные системы реального времени, удовлетворяющие (хотя бы частично) требованиям системы стандартов POSIX, пример - QNX Neutrino v6.2 /2/;
- операционные системы реального времени с уникальной архитектурой, пример -Microware OS-9/9000 /3/;
- SCADA-пакеты, полностью основанные на визуальных и графических языках программирования, пример - National Instruments LabVIEW /4/.

Для всех этих систем была изучена возможность существования КВ на примере так называемых “файловых вирусов” трех типов /5/:

1) перезаписывающих вирусов (overwriting);
2) вирусов-спутников (companion);
3) вирусов-“паразитов”.

Была исследована (см. табл. 1) реализуемость четырех фаз жизненного цикла КВ /6/:

- поиск программного компонента (“жертвы”), пригодного для внедрения в него постороннего программного кода (вируса);
- прикрепление вируса к файловому образу “жертвы”;
- обеспечение несанкционированного получения управления вирусом;
- обеспечение обратной передачи управления программному коду “жертвы”.

Таблица 1

Возможность существования вирусов в различных средах

	Overwriting	Companion	Вирусы-паразиты
OS-9/9000	Да	Да	Да
QNX	Да	Да	Теоретически да /7/
LabVIEW	Да	Да	Нет (?)

С одной стороны, возможность существования КВ во всех случаях основывается на наличии в рассмотренных средах системных средств общего назначения: дисковых и файловых сервисов, средств управления многозадачностью и пр. С другой стороны, эти среды являются узкоспециализированными и поэтому не содержат никаких средств информационной защиты от злонамеренных воздействий. Таким образом, **не существует никаких объективных (в частности, технических) факторов, препятствующих существованию КВ в системах промышленной автоматизации.**

Использование “традиционных” антивирусов (“фагов”, “вакцинаторов”, “сканеров” и пр.) противоречит практически всем требованиям, предъявляемым к системам автоматизации (работа в режиме реального времени, экономия системных ресурсов, непрерывный и циклический алгоритм функционирования и пр.). Наиболее целесообразной представляется методика антивирусной защиты, использующая проверку целостности потенциально уязвимых программных компонентов и, при необходимости, восстановление их из резервной копии. Только одна из рассмотренных сред (OS-9/9000) содержит стандартные средства, которые потенциально могут быть использованы для решения этой задачи (контроль целостности модулей памяти при помощи CRC-12). Тем не менее, их использование стандартизовано и документировано, что позволило КВ легко их нейтрализовать.

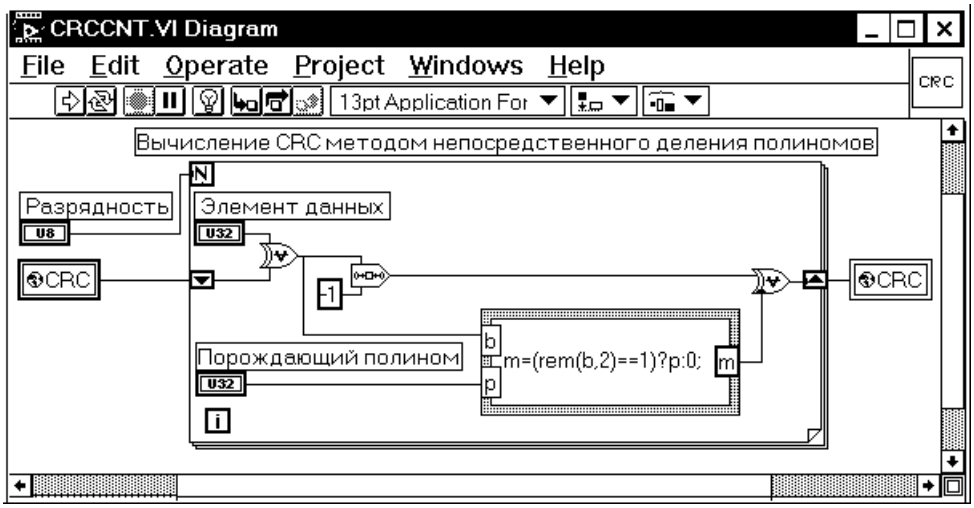

Рис. 1. Виртуальный прибор LabVIEW для расчета CRC

Разработаны и предлагаются к использованию компактные и быстрые средства для проверки целостности компонентов прикладных систем, реализованных в данных средах, а именно: библиотеки процедур для расчета различных хеш-функций (CRC, MD5, хеши группы SHA и т.п.) /8/. Также разработаны библиотеки процедур анализа и тестирования наборов данных с жесткой, заранее известной структурой (баз данных, заголовков и служебных таблиц системных модулей и т.п.). Они могут быть использованы для внешней проверки целостности файлов и областей памяти и для самопроверки программных модулей.

Предполагается продолжить исследования в рамках проблемной области, расширенной за счет:

- SCADA-систем со скриптовыми языками программирования (Wonderware Intouch, AdAdsta TraceMode и пр.);
- рассмотрения сетевых червей и вирусов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Климентьев К.Е.* Обучение методам защиты информации в системах реального времени // Теория и методика непрерывного профессионального образования. Сборник трудов V Всероссийской научно-методической конференции.Том 1. – Тольятти, 2003. - С. 61-63.

2. *Баландин А.В., Николаев А.В.* Основы пользовательской работы в операционной системе QNX. Методические указания. / Самар. гос. Аэрокосм. ун-т. Самара, 2003. – 18 с.

3. *Баландин А.В., Климентьев К.Е.* Организация и функционирование операционной системы реального времени OS-9/9000 / Самара: Университет Наяновой, 1996. – 101 с.

4. *Климентьев К.Е.* Основы графического программирования в среде LabVIEW / Самар. гос. Аэрокосм. ун-т. Самара, 2003. – 79 с.

5. *Касперский Е.В.* Компьютерные вирусы в MS-DOS / М.: “Эдэль”, 1992. – 176 с.

6. *Fred Cohen.* Computer Viruses - Theory and Experiments. Computer Security: A Global Challenge, Elsevier Science Publishers B. V. (North-Holland), 1984. - pp. 143-158.

7. Компьютерные вирусы в UNIX или Гибель Титаника II / В кн. Касперски Крис. Записки исследователя компьютерных вирусов.- СПб.: “Питер”, 2005. – 316 с.

8. *Баричев С.Г., Гончаров В.В., Серов Р.Е.* Основы современной криптографии. – М.: Горячая линия - Телеком, 2002. – 175 с.