УДК 681.3

ОСОБЕННОСТИ АНАЛИЗА ЦЕЛОСТНОСТИ ДАННЫХ

© 2016 П. В. Лобзин

Воронежский институт высоких технологий

В статье рассматриваются особенности анализа целостности данных в информационных системах. Указаны основные аспекты уязвимости информации. Отмечены условия изолированности компьютера.

Ключевые слова: данные, защита, компьютер, уязвимость.

Проблемы защиты информации связаны с ростом возможностей вычислительной техники. Развитие средств, методов и форм автоматизации процессов обработки информации, массовость применения персональных электронно-вычислительных машин (ПЭВМ) резко повышают уязвимость информации.

Защита информации находится в центре внимания не только специалистов по разработке и использованию информационных систем, но и широкого круга пользователей. В последние годы, в связи с широким распространением и повсеместным применением вычислительной техники, массовостью внедрения ПЭВМ, резко повысилась уязвимость накапливаемой, хранимой и обрабатываемой в системах информации. Сейчас четко выделяются три аспекта уязвимости информации:

1) подверженность физическому уничтожению или искажению;

2) возможность несанкционированной (случайной или умышленной) модификации;

3) опасность несанкционированного (случайного или умышленного) получения информации лицами, для которых она не предназначалась.

Приведенные факты показывают, что опасность несанкционированных злоумышленных действий в вычислительных средствах и системах является весьма реальной и с дальнейшим развитием вычислительной техники угроза повреждения информации, несмотря на Все усилия по ее защите, неизменно растет. Все это обусловливает необходимость углубленного анализа опыта защиты информации и комплексной организации методов и механизмов защиты.

Под угрозой безопасности информации понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств. Если исходить из классического рассмотрения кибернетической модели любой управляемой системы, возмущающие воздействия на нее могут носить случайный характер. Поэтому среди угроз безопасности информации следует выделять как один из видов угрозы случайные, или непреднамеренные.

Задача защиты закладок может рассматриваться в принципиально различных вариантах:

- не допустить внедрения программной закладки в компьютерную систему;
- выявить внедренную программную закладку;
- удалить внедренную программную закладку.

При рассмотрении этих вариантов решение задачи защиты от программных закладок сходно с решением проблемы защиты компьютерных систем от вирусов. Как и в случае борьбы с вирусами, задача решается с помощью средств контроля за целостностью запускаемых системных и прикладных программ, а также за целостностью информации, хранимой в компьютерной системе и за критическими для функционирования системы событиями. Однако данные средства действительны только тогда, когда сами они не подвержены влиянию программных закладок, которые могут:

- навязывать конечные результаты контрольных проверок;
- влиять на процесс считывания информации и запуск программ, за которыми осуществляется контроль;
- изменять алгоритмы функционирования средств контроля.

При этом чрезвычайно важно, чтобы включение средств контроля выполнялось до начала воздействия программной закладки либо когда контроль осуществляется только с использованием программ управ-

Лобзин Павел Викторович – ВИВТ АНОО ВО, аспирант, e-mail: LobzPalllodtr1@yandex.ru.

ления, находящихся в ПЗУ компьютерной системы.

1. Защита от внедрения программных закладок. Универсальным средством защиты от внедрения программных закладок является создание изолированного компьютера. Компьютер называется изолированным, если выполнены следующие условия:

- в нем установлена система BIOS, не содержащая программных закладок;
- операционная система проверена на наличие в ней закладок;
- достоверно установлена неизменность BIOS и операционной системы для данного сеанса;
- на компьютере не запускалось и не запускается никаких иных программ,

кроме уже прошедших проверку на присутствие в них закладок;

- исключен запуск проверенных программ в каких-либо иных условиях, кроме перечисленных выше, т. е. вне изолированного компьютера.

Для определения степени изолированности компьютера может использоваться модель ступенчатого контроля. Сначала проверяется, нет ли изменений в BIOS. Затем, если все в порядке, считывается загрузочный сектор диска или драйвера операционной системы, которые, в свою очередь, также анализируются на предмет внесения в них несанкционированных изменений. И, наконец, с помощью операционной системы запускается драйвер контроля вызовов программ, который следит за тем, чтобы в компьютере запускались только проверенные программы.

Интересный метод борьбы с внедрением программных закладок может быть использован в информационной банковской системе, в которой циркулируют исключительно файлы – документы. Чтобы не допустить проникновения программной закладки через каналы связи, в этой системе не допускается прием никакого исполняемого кода. Для распознавания событий типа «ПОЛУЧЕН ИСПОЛНЯЕМЫЙ КОД» и «ПОЛУЧЕН ФАЙЛ-ДОКУМЕНТ» применяется контроль за наличием в файле запрещенных символов: файл признается содержащим исполняемый код, если в нем присутствуют символы, которые никогда не встречаются в файлах-документах.

2. Выявление внедренной программной закладки. Выявление внедренного кода программной закладки заключается в обнаружении признаков его отсутствия в компьютерной системе. Эти признаки можно разделить на следующие два класса:

- качественные и визуальные;
- обнаруживаемые средствами тестирования и диагностики.

К качественным и визуальным признакам относятся ощущения и наблюдения пользователя компьютерной системы, который отмечает определенные отклонения в ее работе (изменяется состав и длины файлов, старые файлы куда-то пропадают, а вместо них появляются новые, программы начинают работать медленнее, или заканчивают свою работу слишком быстро, или вообще перестают запускаться). Несмотря на то, что суждение о наличии признаков этого класса кажется слишком субъективным, тем не менее, они часто свидетельствуют о наличии неполадок в компьютерной системе и, в частности, о необходимости проведения дополнительных проверок присутствия программных закладок.

Признаки, выявляемые с помощью средства тестирования и диагностики, характерны как для программных закладок, так и для компьютерных вирусов. Например, загрузочные закладки успешно обнаруживаются антивирусными программами, которые сигнализируют о наличии подозрительного кода в загрузочном секторе диска. С инициированием статической ошибки на дисках хорошо справляются средства работы с дисковыми накопителями, входящие в Windows. А средства проверки целостности данных на диске, входящие в состав современных антивирусных средств, позволяют успешно выявлять изменения, вносимые в файлы программными закладками. Кроме того, эффективен поиск фрагментов кода программных закладок по характерным для них последовательностям нулей и единиц (сигнатурам), а также разрешение выполнения только программ с известными сигнатурами.

3. Удаление внедренной программной закладки. Конкретный способ удаления внедренной программной закладки зависит от метода ее внедрения в компьютерную систему. Если это программно-аппаратная закладка, то следует перепрограммировать ПЗУ компьютера. Если это загрузочная, драйверная, прикладная, замаскированная закладка или закладка-имитатор, то можно заменить их на соответствующую загрузочную запись, драйвер, утилиту или служебную программу, полученную от источника, заслуживающего доверия. Наконец, если это исполняемый программный модуль, то можно попытаться добыть его исходный текст, убрать из него имеющиеся закладки

или подозрительные фрагменты, а затем заново откомпилировать.

ЛИТЕРАТУРА

1. Чопоров О. Н. Методы анализа значимости показателей при классификационном и прогностическом моделировании / О. Н. Чопоров, А. Н. Чупеев, С. Ю. Брегеда // Вестник Воронежского государственного технического университета. – 2008. – Т. 4. – № 9. – С. 92-94.

2. Душкин А. В. Декомпозиционная модель угроз безопасности информационно-телекоммуникационным системам / А. В. Душкин, О. Н. Чопоров / Информация и безопасность. – 2007. – Т. 10. – № 1. – С. 141-146.

3. Попов Е. А. Риск-анализ информационно-телекоммуникационных систем при аддитивном характере параметра нерегулярности / Е. А. Попов, Н. Н. Корнеева, О. Н. Чопоров, А. В. Заряев // Информация и безопасность. – 2013. – Т. 16. – № 4. – С. 482-485.

4. Калашников А. О. Атаки на информационно-технологическую инфраструктуру критически важных объектов: оценка и регулирование рисков / А. О. Калашников, Е. В. Ермилов, О. Н. Чопоров, К. А. Разинкин, Н. И. Баранников // Монография под ред. чл.-корр. РАН Д. А. Новикова. Воронеж, 2013, Издательство: ООО «Издательство «Научная книга», 159 с.

5. Lvovich Y. E. The use of «ant» algorithm in constructing models of objects that have maximum average values of the scattering characteristics / Y. E. Lvovich, I. Y. Lvovich, A. P. Preobrazhenskiy, O. N. Choporov // Life Science Journal. – 2014. – Т. 12. – № 12. – С. 463.

6. Чопоров О. Н. Рационализация управления региональными системами на основе использования методов системного анализа, информационных и ГИС-технологий / О. Н. Чопоров, Н. А. Гладских, С. С. Пронин, М. И. Чудинов, С. Н. Семенов, К. Л. Матюшевский // Прикладные информационные аспекты медицины. – 2007. – Т. 10. – № 2. – С. 15-19.

7. Зазулин А. В. Особенности построения семантических моделей предметной области / А. В. Зазулин, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2008. – № 3. – С. 026-028.

8. Иванов М. С. Разработка алгоритма отсечения деревьев / М. С. Иванов, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2008. – № 3. – С. 031-032.

9. Зяблов Е. Л. Разработка лингвистических средств интеллектуальной поддержки на основе имитационно-семантического моделирования / Е. Л. Зяблов, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2009. – № 5. – С. 24-26.

10. Львович Я. Е. Адаптивное управление марковскими процессами в конфликтной ситуации / Я. Е. Львович, Ю. П. Преображенский, Р. Ю. Паневин // Вестник Воронежского государственного технического университета. – 2008. – Т. 4. – № 11. – С. 170-171.

11. Львович И. Я. Факторы угрозы экономической безопасности государства / И. Я. Львович, А. А. Воронов, Ю. П. Преображенский // Информация и безопасность. 2006. – Т. 9. – № 1. – С. 36-39.

12. Воронов А. А. Обеспечение системы управления рисками при возникновении угроз информационной безопасности / А. А. Воронов, И. Я. Львович, Ю. П. Преображенский, В. А. Воронов // Информация и безопасность. – 2006. – Т. 9. – № 2. – С. 8-11.

13. Паневин Р. Ю. Реализация транслятора имитационно-семантического моделирования / Р. Ю. Паневин, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2009. – № 5. – С. 57-60.

14. Преображенский Ю. П. Алгоритм нахождения оптимальной стационарной стратегии для марковских процессов принятия решений / Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2010. – № 6. – С. 81-82.

15. Паневин Р. Ю. Представления знаний / Р. Ю. Паневин, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2008. – № 3. – С. 061-064.

THE PECULIARITIES OF ANALYSIS OF DATA INTEGRITY

© 2016 P. V. Lobzin

Voronezh institute of high technologies

The paper considers the peculiarities of analysis of data integrity in information systems. The main aspects of vulnerability information are shown. The conditions of isolation of the computer are marked.

Keywords: data protection, computer, vulnerability.