Технология интеллектуального антивирусного сканирования опасных функций программного обеспечения

А. Л. Огарок,
к.т.н., старший научный сотрудник; специалист по вычислительным системам, синтезирующим системам визуализации, технический директор НПФ «СТОКОНА»

В. В. Насыпный,
д.т.н., профессор, специалист по системам искусственного интеллекта, научный директор НПФ «СТОКОНА»

Д. В. Комашинский,
специалист по математическому и программному обеспечению автоматизированных систем управления; руководитель проекта «Stocona Antivirus»

Современные технологии антивирусной защиты основаны преимущественно на использовании антивирусного сканирования сигнатур (уникальных последовательностей кодов) известных компьютерных вирусов и мониторинга операций, выполняемых запущенными программами. К сожалению, используемые в них методы эвристического анализа выполняемых программами операций не обеспечивают гарантированной защиты от новых типов компьютерных вирусов. Существующие антивирусные программы требуют постоянного пополнения баз вирусных записей данными сигнатур новых вирусов, а решение о степени опасности операций, выполняемых активированными программами, возлагается, как правило, на пользователя. Кроме того, антивирусные мониторы сами подвержены воздействию запущенных на исполнение программ, в том числе вирусов и программных закладок.

Таким образом, принципиальный недостаток концепции построения существующих антивирусных программ состоит в том, что она допускает «заражение» компьютеров новыми, неизвестными вирусами с последующим их лечением разрабатываемыми под эти вирусы антивирусными компонентами.

Еще более трудной задачей является защита от различного вида закладок, которые представляют совокупность команд, скрытно вводимых в программное обеспечение и воздействующих на прикладные программы с привязкой к содержанию данных, команд или алгоритму их выполнения. Эффективных методов защиты от программных закладок до настоящего времени не предложено. Существующие подходы к решению этой проблемы основаны, как правило, на тестировании программ с целью выявления введенных в них закладок. Однако процесс тестирования является во многом субъективным и не гарантирует выявления даже всех ошибок программистов, не говоря об обнаружении изощренно внедренных в программу закладок.

От этих недостатков практически свободна концепция антивирусной защиты, запантетованная и развиваемая НПФ «СТОКОНА». В ее основу положена так называемая технология интеллектуального сканирования опасных функций программного обеспечения. В отличие от известных антивирусных программ данная технология основывается не на поиске известных вирусов и анализе процесса выполнения программ, а на качественно новой концепции — анализе функций программ без их выполнения.

Технология интеллектуального антивирусного сканирования опасных функций программного обеспечения основывается на методическом аппарате эвристического анализа и искусственного интеллекта и предусматривает (рис. 1):

- автоматический экспертный анализ системой искусственного интеллекта файлов программного обеспечения на предмет наличия в них опасных функций (вирусов и программных закладок);
- верификацию выявленных опасных функций на основе соответствующей базы знаний;
- формирование логического вывода об обнаруженных свойствах вирусов и программных закладок;
- автоматическое формирование алгоритмов лечения файлов (то есть деактивации опасных функций).

Технология позволяет обнаружить и обезопасить (деактивировать) все вирусы — в том числе новые, неизвестные — и любые программные закладки.

Перспективность нового концептуального подхода к построению антивирусной защиты состоит в его инвариантности к новым типам вирусов и универсальности. Инвариантность к новым вирусам обусловлена реализацией контроля функций, содержащихся в кодах программ (а не сигнатур известных вирусов), универсальность — тем, что метод может быть использован для контроля любого программного обеспечения до его запуска (автоматическая верификация).

Преимущество данной технологии перед традиционными заключается в обеспечении гарантированной защиты программного обеспечения от всех типов (в том числе новых, неизвестных) компьютерных вирусов и программных закладок. Достигается это, естественно, за счет дополнительных затрат времени на реализацию более сложного алгоритма поиска и верификации опасных функций. Од-

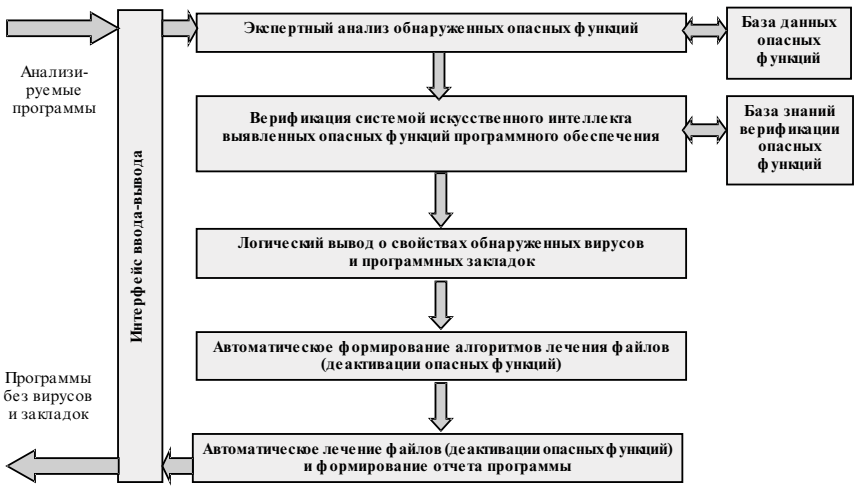

Рис. 1. *Основные положения технологии интеллектуального антивирусного сканирования опасных функций программного обеспечения*

нако эти операции выполняются при открытии потенциально опасных файлов и могут быть реализованы в фоновом режиме.

Работоспособность и эффективность технологии «интеллектуального сканирования» получили всестороннюю проверку и подтверждение на опыте создания компанией «Стокона» (www.stocona.ru) антивирусного программного комплекса (АПК) STOCONA ANTIVIRUS, встраиваемого в Microsoft Office 97/2000/XP. Комплекс осуществляет распознавание и гарантированную защиту компьютера от любых макровирусов и программных закладок.

STOCONA ANTIVIRUS обеспечивает:

- автоматическое определение перечня защищаемых ресурсов компьютерной системы и надежный контроль над всеми программными источниками опасных функций для Microsoft Office и системных ресурсов компьютера;
- гарантированную защиту компьютера от всех макровирусов и программных закладок в документах Microsoft Word, книгах Microsoft Excel и презентациях Microsoft PowerPoint в реальном масштабе времени;
- автоматическую защиту компьютера от любых вирусов и программных закладок во всех входящих и исходящих сообщениях электронной почты Microsoft Outlook;
- эффективное лечение документов Microsoft Word, книг Microsoft Excel, презентаций Microsoft PowerPoint и почтовых сообщений Microsoft Outlook от всех макровирусов и программных закладок;
- надежный контроль целостности и полную автоматизацию процесса защиты системных ресурсов компьютерных систем и программ Microsoft Office от макровирусов и программных закладок.

Гарантией защиты компьютера от всех макровирусов и программных закладок в документах Microsoft Office 97/2000/XP является отключение возможности выполнения неизвестных макросов до проведения их проверки. Процесс их лечения полностью автоматизирован и может быть настроен под требования конкретного пользователя. При необходимости программа позволяет восстановить исходное состояние деактивированных опасных макросов.

Система чрезвычайно проста в эксплуатации и после установки не требует от пользователя никаких усилий («установил и забыл»). При этом пользователь полностью освобождается от неприятной необходимости постоянного обновления баз вирусных записей.

Сравнительный анализ основных характеристик АПК STOCONA ANTIVITUS с наиболее известными антивирусными программами приведен в таблице 1.

В ближайшее время компания «Стокона» завершает разработку и планирует начать поставку на рынок АПК «STOCONA ANTIVIRUS» для полного комплекта приложений Microsoft Office XP и для броузеров Microsoft Internet Explorer, Netscape Navigator и почтовых пакетов Outlook Express и Lotus.

Непосредственное встраивание интеллектуального антивирусного сканера в прикладные программные комплексы широкого применения (например, Microsoft Office, Star Office, Autocad, Бухгалтерия 1С и другие) составляет, очевидно, одно из наиболее перспективных направлений реализации технологии. Такой подход, по-видимому, можно считать оптимальным, так как он обеспечивает исключение избыточности базы данных потенциально опасных функций и базы знаний их верификации, которая неизбежно имела бы место при создании универсального (по отношению к прикладным программам) сканера.

По нашему убеждению, встраивание интеллектуального антивирусного сканера опасных функций в существующие прикладные программные комплексы обеспечивает полное решение антивирусной защиты этих приложений и исключает необходимость применения для их защиты антивирусных программ сторонних производителей.

Таблица 1

Сравнительный анализ основных характеристик антивирусного программного комплекса STOCONA ANTIVIRUS с наиболее известными антивирусными программами

Анализируемые характеристики антивирусной защиты Microsoft Office	**Антивирусные программы**				
	AVP Personal Pro (Office Guard, MailChecker)	**DrWeb**	**Norton Antivirus 8.0**	**«TREND MICRO» OfficeScan Corporate Edition**	**Stocona Antivirus 2.0**
Обнаружение компьютерных вирусов в документах Microsoft Office	Обеспечивается обнаружение известных макровирусов и многих (порядка 80%) опасных функций новых макровирусов	Обеспечивается обнаружение известных макровирусов и некоторых (около 5%) опасных функций новых макровирусов	Обеспечивается обнаружение известных макровирусов и некоторых (примерно 3%) опасных функций новых макровирусов	Обеспечивается обнаружение известных макровирусов и некоторых (не более 5%) опасных функций новых макровирусов	Обеспечивается обнаружение любых макровирусов, в том числе новых, неизвестных, и всех (100%) опасных функций
Обнаружение программных закладок	Нет. Программные закладки не обнаруживаются				Да. Гарантированное обнаружение любых программных закладок
Реализуемая антивирусная технология	Мониторинг опасных функций, запущенных на выполнение макросов				Интеллектуальное антивирусное сканирование опасных функций и их верификация
Уровень безопасности Microsoft Office	Устанавливается пользователем, по умолчанию «средний»				Устанавливается автоматически «высокий» уровень безопасности
Выполнение автоматических макросов	Возможно				Возможно только для проверенных макросов или при отключении антивирусной защиты конкретного приложения Microsoft Office

Контроль функциональности приложений Microsoft Office	Отсутствует. Возможность неконтролируемой подмены автофункций в макросах может привести к потере функциональности приложений Microsoft Office				Полный контроль функциональности приложений Microsoft Office и защищаемых системных ресурсов компьютера (файлов Windows и Microsoft Office)
Методы противодействия макровирусам	Прерывание опасной операции, переименование файла документа, перемещение файла документа, удаление файла документа	Переименование файла документа, перемещение файла документа, удаление файла документа	Переименование файла документа, перемещение файла документа, удаление файла документа, удаление всех макросов из документа		Лечение документов путем деактивации опасных функций
Вероятность «ложных тревог»	Высокая. Не отслеживается синтаксис и параметры опасных функций		Высокая. Не отслеживается синтаксис и параметры опасных функций. Срабатывает на деактивированные опасные функции		Низкая. Ложные тревоги практически исключены
Степень интеллектуальности программы	Низкая. Производится только обнаружение многих (не более 80%) опасных функций. Их верификация отсутствует			Низкая. Производится обнаружение только некоторых (не более 5%) совокупностей опасных функций. Не считает опасным использование функции в отдельности. Верификация опасных функций отсутствует	Высокая. Производится обнаружение всех опасных функций и их верификация на основе базы знаний
Логический вывод о свойствах макроса	Отсутствует				Интегральный вывод о типе макроса (вируса или программной закладки), о механизмах опасных воздействий
Диалог с пользователем	Выдается текущая обнаруженная опасная функция и запрос на реакцию пользователя (в зависимости от настроек)	Выдается только предупреждение о возможной опасности и запрос на реакцию пользователя (в зависимости от настроек)			Выдается перечень опасных функций, автоматических функций, обнаруженных механизмов воздействия и запрос на проведение лечения (в зависимости от настроек)
Количество обнаруживаемых опасных функций	Выявляется только текущая функция во время выполнения макроса	Выявляются только функции, относящиеся к работе с программным кодом модуля макроса			Выявляются все опасные функции
Автоматический анализ вложенных сообщений Microsoft Outlook	Обнаружение производится только известных макровирусов приложением Mail Checker	Не производится	Производится с тем же уровнем интеллектуальности		Гарантированная защита от запуска любых вирусов и программных закладок, автоматическое лечение вложенных документов Microsoft Office (Word, Excel, PowerPoint)
Автоматический анализ скриптов в теле сообщения Outlook	Автоматическое обнаружение и деактивацая скриптов в теле сообщения	Нет. Скрипты в теле сообщения не анализируются			Автоматическое обнаружение и деактивацая скриптов в теле сообщения
Лечение документов Microsoft Office	Нет. Антивирусные мониторы принципиально не обеспечивают лечение. Сохраняется вероятность заражения других компьютеров невылеченными макровирусами и нанесение деструктивных воздействий программными закладками		Да. Обеспечивается только удаление всех подозрительных макросов из документов Microsoft Office		Да. Обеспечивается гарантированное лечение документов Microsoft Office от макровирусов (в том числе от неизвестных) и от программных закладок
Поддержка актуальности антивируса	Требуется постоянное обновление баз данных сигнатур известных вирусов				Не требуется обновление базы данных опасных функций и базы знаний их верификации

Примечание. Количественные показатели тестов получены на основании составленного нами полного перечня опасных функций макросов в документах Microsoft Office. Низкие показатели количества обнаруживаемых опасных функций в существующих антивирусных программных комплексах обусловлены их ориентацией на обнаружение сигнатур (уникальных байтовых последовательностей) известных макровирусов.