времени выполнения MPI-версии также выше, чем при других подходах. Таким образом, если задача распределена более, чем между 16 процессами, MPI производит самое быстрое решение для используемого набора тестов. Однако MPI – низкоуровневый язык в терминах параллельного программирования. Это "ассемблер" для параллельного программирования, и наиболее трудоемкой частью является этап распределения данных и построения схемы связей между процессами. В некоторых случаях, когда число процессоров меньше 16, рекомендуется применять другие технологии, такие как OpenMP или DVM, которые, хотя и уступают по скорости MPI, являются более легкими для использования и требуют гораздо меньше временных затрат на разработку.

Сравнение на базе NPB 2.3 тестов не может быть всесторонним, так как эти тесты разработаны на очень высоком уровне командой экспертов, но оно может дать общее представление о возможностях рассмотренных параллельных технологий.

Практическая значимость. Параллельные программы требуют значительных модификаций на этапе разработки и использования для оптимизации вычислительных показателей. В этой связи результаты, полученные в работе, могут быть использованы как практические рекомендации разработчику параллельных приложений.

Литература: 1.*Michael Frumkin*, Haoqiang Jin and Jerry Yan (1998). Implementation of NAS Parallel Benchmarks in High Performance Fortran. NAS Technical Report NAS-98-009, NASA Ames Research Center, 10 p. **2.** *Jin H., Frumkin M. and J. Yan* (1998). The OpenMP Implementation of NAS Parallel Benchmarks and Its Performance. NASA Ames Research Center, 26 p. **3.** *Крюков В.А.* Разработка параллельных программ для вычислительных кластеров и сетей. 2002. Институт прикладной математики им. М.В. Келдыша, РАН. 22 с. **4.** *Bailey D., Harris T., Sahpir W., van der Wijngaart R., Woo A., Yarrow M.* December 1995. The NAS Parallel Benchmarks 2.0. Report NAS-95-020. 24 p. **5.** *Koelbel C.H.* November 1997. An Introduction to HPF 2.0. High Performance Fortran – Practice and Experience. Supercomputing 97. 27 p. **6.** *Koelbel C.H., Loverman D.B., Shreiber R., Steele Jr. GL., Zosel M.E.* 1994. The High Performance Fortran Handbook. MIT Press. 262 p. **7.** *OpenMP* Fortran Application Program Interface, http://www.openmp.org. **8.** *DVM*. Execution performance of NAS tests, http://www.keldysh.ru/dvm/. **9.** *Writing* Message-Passing Parallel Programs with MPI. http://www.epcc.ed.ac.uk/computing/training/document_archive/mpi-course/mpi-course.book_1.html. 10.HP MPI User's Guide. Fourth Edition http://www.docu.sd.id.ethz.ch/comp/stardust/SW/mpi/title.html.

Поступила в редколлегию 05.12.2006

Рецензент: д-р техн. наук, проф. Кривуля Г.Ф.

Горбачев Валерий Александрович, профессор каф. ЭВМ ХНУРЭ. Научные интересы: моделирование систем. Хобби: компьютеры, волейбол, автомобили. Адрес: Украина, 61166, Харьков, пр.Ленина, 14, тел. +38(057)7021-115.

Гриценко Тарас Васильевич, ааспирант каф. ЭВМ ХНУРЭ. Научные интересы: моделирование систем, программирование,параллельные вычисления. Хобби: компьютеры, автомобили. Адрес: Украина, 61166, Харьков, пр.Ленина, 14, тел. +38(057)7021-354.

УДК519.713

ПРОБЛЕМЫ АНТИВИРУСНОЙ ИНДУСТРИИ, МЕТОДЫ БОРЬБЫ С КОМПЬЮТЕРНЫМИ УГРОЗАМИ И БЛИЖАЙШИЕ ПЕРСПЕКТИВЫ РАЗВИТИЯ

ГОРОБЕЦ А.А., КУНИЦКИЙ А.В., ПАРФЕНТИЙ А.Н., ЧУВИЛО О.А.

Исследуется состояние мирового рынка антивирусной индустрии, применяемые технологии борьбы с различными компьютерными угрозами, выявляются проблемы, стоящие перед создателями антивирусных продуктов, и тенденции развития средств борьбы с компьютерными угрозами на ближайшую перспективу.

1. Введение

Цель работы – исследовать рынок средств борьбы с вирусной угрозой, сами антивирусные технологии для выявления в них узких мест (недостатков, проблем), что является необходимым для совершенствования этих технологий.

Задачи исследования – выявить приоритетные направления развития антивирусных технологий и ближайшие перспективы развития антивирусной индустрии.

Объективно сложившаяся обстановка в сфере функционирования компьютерных технологий такова, что постоянные вирусные и троянские атаки терроризируют практически всех пользователей Internet – домашних, небольшие и средние компании, глобальные корпорации и государственные структуры и таким образом оказывают серьезное деструктивное влияние на всю мировую экономику. В настоящий момент уже ясно, что основной целью современных создателей вирусов является извлечение нелегальной прибыли путем создания и распространения вредоносных программ, с помощью которых происходит: воровство частной и корпоративной банковской информации (получение доступа к банковским счетам персональных пользователей и организаций); воровство номеров кредитных карт; распределенные сетевые атаки (DDoS-атаки) с последующим требованием денежного выкупа за прекращение атаки (современный компьютерный вариант обычного рэкета); создание сетей троянских прокси-серверов для рассылки спама (и коммерческое использование этих сетей); создание зомби-сетей для многофункционального использования; создание программ, скачивающих и устанавливающих системы показа нежелательной рекламы; внедрение в компьютеры троянских программ, постоянно звонящих на платные (и весьма дорогие) телефонные номера; иные действия, связанные с возможным

извлечением нелегальной прибыли [2]. В этой связи необходимо адекватно реагировать на возрастающие вирусные угрозы.

2. Анализ состояния рынка мировой антивирусной индустрии, технологий антивирусной защиты

Данное исследование посвящено изучению существующих продуктов антивирусных компаний, применяемых в них технологий и их сравнение. С этой целью рассмотрим примерную расстановку сил компаний, присутствующих на рынке антивирусных технологий, поскольку эта расстановка позволяет определить доминирование тех или иных технологий в антивирусной индустрии, носителями которых являются данные компании. Крупные компании первого эшелона, оборот программных антивирусных продуктов которых составляет более 500 млн долларов США в год, представлены в табл. 1.

Крупные компании второго эшелона, оборот программных антивирусных продуктов которых составляет более 20 млн долларов США в год, представлены в табл. 2.

Таблица 1

Компания	Оборот, млн USD	
	2003	2004
Symantec	1098	1364
McAfee (NAI)	577	597
Trend Micro	382	508

По аналитическим данным «Лаборатория Касперского» также входит во второй эшелон антивирусных

Таблица 2

Компания	Оборот, млн USD	
	2003	2004
Sophos (Англия)	97	116
Panda Software (Испания)	65	104
Computer Associates (США)	61	74
F-Secure (Финляндия)	36	51
Norman (Норвегия)	23	31
AhnLab (Южная Корея)	21	28

компаний, однако свои финансовые показатели компания пока не раскрывает.

Компании третьего эшелона, заметные на мировом рынке программных антивирусных продуктов:

– Alwil – Awast (Чехия)

– Arcabit – MKS (Польша)

– Doctor Web – DrWeb (Россия)

– ESET – NOD32 (Словакия)

– Frisk Software – F-Prot (Исландия)

– GriSoft – AVG (Чехия)

– H+BDV – AntiVir (Германия)

– Hauri – VI Robot (Южная Корея)

– SoftWin – BitDefender (Румыния)

– VirusBuster – VirusBuster (Венгрия).

Первым ответом на возрастание вирусных угроз стало внедрение практически всеми антивирусными разработчиками в своих продуктах различных технологий проактивной защиты. К ней относятся следующие технологии антивирусной защиты: эвристический анализатор; безопасность на основе политик; системы предотвращения вторжений (IPS - Intrusion Prevention System); защита от переполнения буфера (Buffer Overrun); поведенческие блокираторы.

Основой проактивной защиты являются *эвристические анализаторы*, суть которых – набор подпрограмм, анализирующих код исполняемых файлов, макросов, скриптов, памяти или загрузочных секторов для обнаружения в нем разных типов вредоносных компьютерных программ, не определяемых обычными (сигнатурными) методами. Другими словами — эвристические анализаторы предназначены для поиска неизвестного вредоносного ПО [6]. Данная технология может быть использована во всех антивирусных продуктах, как на рабочих станциях, так и на файловых, почтовых серверах и Internet-шлюзах. На сегодняшний день эвристический анализатор — единственная проактивная технология, которая может эффективно использоваться во всех антивирусных продуктах. Обычно эвристические анализаторы располагаются на периметре сети - между компанией и Internet и отслеживают сетевой трафик на наличие признаков атак. Внутри же сети эвристические анализаторы отслеживают поведение программных кодов на компьютере и пытаются блокировать любые программы, действия которых покажутся им вредоносными или подозрительными. Различные антивирусные компании имеют свои собственные эвристические анализаторы, или наборы подпрограмм, которые можно охарактеризовать как собственные технологии, поскольку в них реализованы свои «фирменные алгоритмы». Уровень детектирования у собственно эвристических анализаторов на сегодняшний день не очень высок, так как существуют десятки различных методов их «обмана», которыми пользуются авторы вирусов. Кроме этого, для эвристических анализаторов с высоким уровнем обнаружения характерен высокий уровень ложных срабатываний. Несмотря на невысокий уровень обнаружения, эвристические методы остаются востребованными в современных антивирусах. Причина проста — комбинация различных методов превентивного обнаружения (в частности, метода защиты от переполнения буфера и поведенческого блокиратора) приводит к повышению его качества [3].

Системы предотвращения вторжений (Intrusion Prevention System - IPS) предусматривают возможность закрытия наиболее часто используемых вредоносными программами уязвимостей компьютера перед новой угрозой еще до выхода обновления антиви-

русных баз: блокировка портов, т.е. блокируется возможность попадания инфекции на компьютер и ее дальнейшего размножения; создание политик для ограничения доступа к директориям или отдельным файлам; обнаружение источника инфекции в сети и блокировка дальнейших коммуникаций с ним. Данная технология отлично работает против атак хакеров и бесфайловых червей и вирусов. Однако против почтовых червей, классических вирусов и троянских программ IPS не эффективна.

Защиту от переполнения буфера также можно отнести к элементам проактивной защиты, так как при большинстве современных атак задействуются различные уязвимости, использующие переполнение буфера, а эта технология просто исключает применение такой уязвимости любым вредоносным кодом или атакой. С учетом того, что все современные процессоры поддерживают на аппаратном уровне защиту от переполнения буфера, перспективность программной реализации сомнительна. Но тем не менее, защита от переполнения буфера востребована для защиты рабочих станций, Internet-шлюзов и других серверов, которые имеют прямой выход в Internet.

К проактивной защите также относят и современные *поведенческие блокираторы*. Основная идея блокиратора – анализ поведения программ и блокировка выполнения любых опасных действий. Теоретически блокиратор может предотвратить распространение любого, как известного, так и неизвестного (написанного после блокиратора) вируса. Именно в этом направлении и движется большинство разработчиков антивирусного ПО. Поведенческие блокираторы применимы только в случаях, когда возможно исполнение подозрительной программы — на рабочих станциях. На почтовых, файловых серверах и шлюзах запуск подозрительных программ не должен осуществляться в принципе и, как следствие, поведенческий блокиратор не будет востребован. Компания *Symantec* в качестве проактивной защиты использует встроенный эвристический анализатор, способный обнаруживать еще не известные модификации вирусов на основании их специфических действий в системе, а также компоненты IPS/IDS (Intrusion Prevention/ Detection System) *Norton Internet Worm Protection*, позволяет закрыть наиболее распространенные пути инфекции в систему (Prevention) и детектировать подозрительные действия (Detection). Компания *McAfee* также активно развивает методы проактивной защиты в своих продуктах семейства McAfee Entercept. Кроме этого, продукты не допускают переполнения буфера для примерно 20 наиболее распространенных программ и сервисов Windows, включая Word, Excel, Internet Explorer, Outlook и SQL Server, что также можно отнести к проактивной защите. Кроме того, используется эвристическая технология *WormStopper*. Компания *Trend Micro* в качестве проактивной защиты *PC-cillin Internet Security 2005* использует эвристический анализатор и *Outbreak Alert System* — проактивное оповещение о новых наступающих угрозах. Компания *Sophos* имеет технологию IPS, которая расшифровывается как “Intrusion Prevention System” – система предотвращения вторжения. Компания *Panda Software* имеет технологию *TruPrevent*™, которая включает в себя три компонента: поведенческий анализатор процессов для исследования поведения запущенных в системе процессов и обнаружения подозрительных действий, эвристический анализатор и набор IDS-функций для обнаружения вредоносных сетевых пакетов и защиты от переполнения буфера. Продукт позиционируется компанией Panda Software как вторая линия обороны от любого неизвестного вредоносного ПО (в качестве первой линии должен выступать классический антивирус) и предназначен для обнаружения неизвестного malware, запускаемого на компьютере. Достоинством является возможность ее работы вместе с антивирусами других производителей. Компания *«Лаборатория Касперского»* – в 6-й версии своих продуктов внедрила модуль проактивной защиты KIS, который включает в себя как уже хорошо зарекомендовавшие себя технологии, так и ряд новых разработок. В новых продуктах от «Лаборатории Касперского» наряду с зарекомендовавшим себя эвристическим анализатором объединен ряд новейших технологий проактивной защиты. В продуктах используется и система обнаружения и предотвращения вторжений *(IPS/IDS)*, направленная на борьбу с хакерскими атаками и бесфайловыми вирусами. Система *нотификации* позволяет предупреждать пользователей об эпидемиях и других событиях, касающихся безопасности. Но наиболее важным нововведением, с точки зрения борьбы с новыми угрозами, является поведенческий блокиратор второго поколения. Данный блокиратор отличает важная особенность — «откат» действий, совершенных вредоносным кодом. Это позволяет значительно сократить количество вопросов пользователю и уменьшить риск повреждения системы до детектирования нового вредоносного ПО. Компания *ESET* обладает патентованной технологиией *ESET ThreatSense*, которая на уровне ядра антивирусной программы позволяет производить глубокий эвристический анализ кода. Компания *SoftWin* в продуктах *BitDefender* в качестве проактивной защиты использует поведенческий анализатор, который блокирует вредоносные программы на основании анализа их специфических действий в системе (контролируются системные файлы, реестр и Internet-активность).

Для защиты почтового трафика могут использоваться особые методы проактивной защиты, основанные на анализе писем, проходящих через почтовый сервер. С помощью такого анализа можно остановить эпидемию в самом ее начале. Статистика, дающая основания подозревать начало эпидемии, может быть следующей: массовая рассылка или прием одинаковых вложений; массовая рассылка или прием одинаковых писем с различными вложениями; наличие двойного расширения у вложений. Кроме этого, возможен лингвистический анализ тел писем.

Сводные данные по применению различных проактивных технологий ведущими компаниями-разработчиками приведены в табл. 3.

Суммируя все сказанное выше, можно говорить о том, что под проактивными методами защиты, предлагаемыми на рынке, понимается: поведенческий анализатор процессов для анализа поведения запущенных в системе процессов и обнаружения подозрительных

Таблица 3

	MA	Sym	TrM	ЛК
Эвристический анализатор	+	+	+	+
Сист. предотвращения вторжений	+	+	-	+
Защита от переполнения буфера	+	-	-	-
Безопасность на основе политик	-	-	+	-
Оповещение о новых угрозах	-	+	+	+
Поведенческий блокиратор	-	-	-	+

действий, т. е. неизвестных вредоносных программ; устранение возможностей попадания инфекции на компьютер, блокировка портов, которые используются уже известными вирусами и могут использоваться их новыми модификациями (IPS/IDS-компонент); недопущение переполнения буфера для наиболее распространенных программ и сервисов Windows, чаще всего используемых злоумышленниками для осуществления атаки (IPS/IDS-компонент); минимизация ущерба, причиненного инфекцией, предотвращение дальнейшего ее размножения, ограничение доступа к файлам и директориям; обнаружение и блокировка источника инфекции в сети (IPS/IDS-компонент). Технологии проактивной защиты на сегодняшний день являются приоритетным направлением работы для компаний-разработчиков антивирусного ПО [3].

На данный момент неотъемлемой частью антивирусного ПО является сканер, выполняющий сигнатурный анализ файлов. Суть работы сканера заключается в поиске в файлах, памяти и загрузочных секторах вирусных масок (сигнатур) - уникального программного кода вируса. Вирусные маски (сигнатуры) известных вирусов содержатся в антивирусной базе данных и если сканер встречает программный код, совпадающий с одним из этих описаний, то он выдает сообщение об обнаружении соответствующего вируса [10]. Другим аспектом данной проблемы являются так называемые полиморфные вирусы, т.е. вирусы, не имеющие постоянного программного кода: заражая очередной файл, они при помощи шифрования самостоятельно изменяют свой вид, при этом сохраняя свою функциональность. Сканеры также делятся на «резидентные» (мониторы), производящие сканирование «на лету», и «нерезидентные», обеспечивающие проверку системы только по запросу. К недостаткам таких сигнатурных сканеров можно отнести размеры антивирусных баз, которые сканерам приходится все время пополнять и обновлять, поскольку малейшие модификации вируса могут сделать его невидимым для сканера: программный код не будет полностью совпадать с описанием в базе данных. Кроме того, у сканеров достаточно высокая требовательность к системным ресурсам и небольшая скорость поиска вирусов.

Существуют также сканеры контрольных сумм (CRC-сканеры), принцип работы которых основан на подсчете контрольных сумм для присутствующих на диске файлов/системных секторов. Эти контрольные суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т.д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом. Однако у CRC-сканеров есть существенный недостаток, состоящий в том, что они не способны поймать вирус в момент его появления в системе, а делают это лишь через некоторое время, уже после того, как вирус разошелся по компьютеру. Кроме того, периодически появляются вирусы, которые заражают только вновь создаваемые файлы и остаются, таким образом, невидимыми для CRC-сканеров.

3. Принципы предотвращения вирусных угроз

По принципам предотвращения вирусных угроз программные средства борьбы можно разделить следующим образом:

1) *Сигнатурный анализ* – основной принцип антивирусных пакетов. При своевременном обновлении баз вирусных сигнатур пакеты, основанные на этом принципе, способны выявлять и блокировать вредоносные коды на стадии их внедрения в атакуемый компьютер.

2) *Блокирование трафика, генерируемого троянскими программами, и команд управления, посылаемых злоумышленником* - основной принцип, используемый персональными и централизованными межсетевыми экранами.

3) *Блокирование запуска программ, явно не указанных как разрешенные* - основной принцип, используемый средствами контроля запуска приложений.

4) *Контроль за своевременной установкой заплат и исправлений к ПО* - основной принцип, используемый в программных пакетах, которые позволяют своевременно устанавливать выпускаемые производителем исправления и заплатки, и тем самым устраняют уязвимости приложений, используемые для внедрения вредоносных кодов [4].

4. Основные проблемы антивирусной индустрии

1) Все возрастающее количество и разнообразие вредоносных программ.Многие антивирусные компании просто не в состоянии угнаться за этим потоком, они проигрывают в вирусной «гонке вооруже-

ний», а пользователи этих программ оказываются защищены далеко не от всех современных компьютерных угроз. Вследствие этого необходимо искать новые методы быстрого обнаружения различных вредоносных угроз [1].

2) Повсеместное внедрение Internet, используемого в качестве транспорта для различных вредоносных угроз и как следствие – колоссальное ускорение распространения этих угроз.

3) Необходимость эффективного удаления обнаруженного вредоносного кода из зараженной системы, поскольку часто вирусы и троянские программы предпринимают специальные действия, чтобы скрыть факт своего присутствия в системе. И чем тщательнее проверяются файлы, тем больше съедается ресурсов компьютера.В результате появляется следующая проблема – проблема баланса.

4) Проблема - баланс между обеспечением полноценной защиты и более высокой скоростью работы антивирусной программы. Эту проблему можно обозначить и так: целесообразность потребления ресурсов защищаемого компъютера при осуществлении этой защиты.

5) Технологическая исключительность, т.е. несовместимость различных антивирусных программ между собой, что приносит больше вреда, чем пользы в борьбе с вирусной угрозой [7].

5. Заключение

Следует отметить, что не существует антивирусов, гарантирующих стопроцентную защиту от вирусов [8]. Более того, невозможность существования абсолютного антивируса была доказана математически на основе теории конечных автоматов Фрэдом Коэном, автором термина “компьютерный вирус”[11]. Однако очевидно, что с нарастанием вирусных угроз методы антивирусной борьбы должны совершенствоваться, чтобы адекватно реагировать на эти угрозы.

Наиболее эффективны в борьбе с компьютерными вирусами антивирусные программы. Однако на сегодняшний день ясно, что методы борьбы становятся все более комплексными, т.е. все шире применяются не только чисто программные методы (различные антивирусные пакеты и более совершенные технологии в этих пакетах), но и технические и организационные методы.

Совершенствование компьютерных технологий, появление многоядерных процессоров и, как следствие этого, активное применение технологий виртуализации позволили дополнить технологии антивирусной борьбы новыми техническими средствами, которые в свою очередь дают возможность по-новому строить системы защиты организационно [5]. Речь идет о новом подходе компании Intel , который уже реализован в их чипсетах и доступен к массовому применению. Технические возможности новых чипсетов позволяют разделить функционально одну физическую машину на несколько виртуальных, придав им различные функции. Разделение на виртуальные машины несет в себе кроме технического и организационный аспект построения сети. Первая виртуальная машина конфигурируется для осуществления выхода в сеть. На ней устанавливается жесткий набор приложений, связанных с фильтрацией сетевых пакетов, почты, и антивирусные пакеты, которые анализируют весь входящий трафик на наличие различных компьютерных угроз. При этом на уровне чипсета этой виртуальной машине «отдается» управление сетевой картой и отдельная область памяти. Кроме того, поскольку в приложениях после их инсталляции и настройки ничего не меняется, то на уровне чипсета проверяются записанные контрольные суммы этих приложений. Любое повреждение приложений, вплоть до искусственного внедрения вируса приведет к блокированию работы виртуальной машины, отвечающей за работу с внешним периметром сети. Восстановление «чистой» виртуальной машины не представляет ни технических, ни особых временных затрат. Остальные виртуальные машины настраиваются на работу с приложениями, соответствующими профилю деятельности компании, и соответственно, их количество определяется исходя из мощности физической машины. Кроме того, частью технологий, внедренных в этот же чипсет, является удаленное администрирование рабочими станциями. Повышение безопасности с точки зрения устойчивости сети к различным вторжениям здесь проявляется в возможности из единого административного центра реализовывать быстро и эффективно политику безопасности на распределенных участках корпоративной сети [9].

В частности, это может быть регулярное обновление образа системы и приложений на рабочих станциях администратором удаленно, что может быть принято в качестве организационных мер (политики) против различных вторжений, когда они происходят, скажем, изнутри сети (к примеру, по нерадивости сотрудника).

Однако применение новых беспроводных технологий несет с собой изменения в организации корпоративных сетей, сутью которых является появление все больших уязвимостей в периметре сети. Если раньше выход во внешнюю сеть Internet осуществлялся через один шлюз, а все компьютеры, работающие в корпоративной сети, находились в пределах ее периметра, то применение этих технологий может привести к тому, что достаточно существенная часть «своих» компьютеров может то входить в периметр сети, то выходить из него. Периодический вход и выход из корпоративной сети характерен для различных мобильных устройств, оснащенных беспроводными интерфейсами. Причем каждый очередной вход потенциально может нести вирусную угрозу, поскольку за пределами периметра компьютер находится вне зоны действия корпоративной системы безопасности. Это обстоятельство на порядок усложняет систему организации безопасности сети.

В этом случае применяются системы управления безопасностью на основе тех же антивирусных пакетов, дополненных мощной системой администрирования при управлении безопасностью корпоративной сети. В частности, такими функциями обладают продукты компании *McAfee*, которые могут управлять безопасностью сетей с количеством *десятков и даже сотен тысяч компьютеров*. При применении такой системы безопасности никакой компьютер не может быть допущен в сеть без принудительного внедрения в него антивирусного агента и проведения соответствующей антивирусной обработки. При этом следует сказать, что внедрение новых технологий, связанных с увеличение количества ядер в процессоре, а также технологий виртуализации, реализованных на уровне чипсета, уже в 2007 году коснутся и мобильных устройств. Это позволит на уровне мобильных устройств организовывать первую линию защиты на основе виртуальной машины, что в свою очередь упростит общее управление безопасностью корпоративной сети при входе такого устройства в сеть по беспроводному интерфейсу.

Что касается развития собственно программных средств противостояния внешним угрозам, то, очевидно, их направление развития в ближайшем будущем лежит в области совершенствования алгоритмов проактивной защиты в целях повышения распознавания угроз и уменьшения ложных срабатываний. В связи с этим предлагается в качестве направления разработки совершенствование алгоритмов анализа вида программы и ее кода с тем, чтобы определить, как программа была создана, и алгоритмов определения типа поведения кода и что он будет пытаться сделать в случае исполнения. Предлагается также шире использовать технические средства, например, делать прошивки антивирусных программ в программируемые логические матрицы и встраивать их в различные устройства (контроллеры, мобильные платежные системы), которые помимо компьютера имеют возможность самостоятельно выходить в Internet и, соответственно, становятся потенциальными объектами вирусных атак. Только применение всех методов борьбы в комплексе позволит адекватно противостоять вирусным угрозам.

Научная новизна работы состоит в предложении применения комплексного подхода к защите от вирусных угроз, заключающегося в применении технических, программных и организационных мер, а также совершенствования алгоритмов проактивной защиты для уменьшения количества ложных срабатываний в компьютерных системах. Это позволит применять их в различных устройствах (контроллеры, мобильные платежные системы), имеющих самостоятельный выход в Internet, путем прошивки этих алгоритмов в схемотехнические решения, например в программируемые логические матрицы. Это позволит защитить нарождающийся массовый рынок таких устройств от возможных вирусных атак.

Практическая значимость результатов исследования определяется возможностью их использования компаниями-разработчиками антивирусного ПО при выборе приоритетного направления совершенствования своей продукции, что позволит им освоить новый сегмент рынка. Кроме того, эти результаты применимы для использования различными компаниями при организации защиты своих компьютерных сетей от вирусных угроз.

Литература:1. *Касперский Е.* Современная антивирусная индустрия и её проблемы, 2005. http://www.viruslist.com/ru/analysis?pubid=174261388 **2.** *Касперский К.* Записки исследователя компьютерных вирусов. СПб.:Питер, 2005. 316 с. **3.** *Никишин А.* Проактивная защита как она есть, 2005.http://www.viruslist.com/ru/analysis?pubid=170273483 **4.** *Вируспосиатели* меняют тактику. http://www.bms-consulting.com/ru/press/news/experience_box/6/ **5.** *IDF*: Microsoft и Intel рассказали о сотрудничестве в области виртуальных технологий, 2006. http://www.cybersecurity.ru/hard/8488.html?page=1 **6.** *Доля А.* Проактивные технологии для борьбы с вирусами. http://www.compdoc.ru/secur/virus/proaktiv_tech/ **7.** *Microsoft* откроет доступ к ядру Windows Vista, 2006. http://www.antimalware.ru/index.phtml?part=news&newsid=252&arc=1 **8.** *Крюков А.* Антивирусные программы. http://beda.stup.ac.ru/psf/ziss/wmaster/books/other/avpve/2METHOD/22-ANTIV/22-ANTIV.htm **9.** *Компьютерные* вирусы и антивирусные программы http://iomas.vsau.ru/uch_proz/ei/txt/internet/leture_virus.htm **10.** *Антивирусная* защита. Типы антивирусных программ. http://1c-audit.ru/modules/news/article.php?storyid=81 **11.** *Исследование* Фрэда Коэна http://www.phreaking.ru/showpage.php?pageid=54088.

Поступила в редколлегию 02.12.2006

Рецензент: д-р техн. наук, проф. Хаханов В.И.

Горобец Александр Александрович, студент факультета Компьютерной инженерии и управления (каф. электронных вычислительных машин) ХНУРЭ. Научные интересы: анализ вредоносного кода. Адрес: Украина, 61174, Харьков, пр. Л. Свободы , 60, кв.27, тел. 80674174546.

Куницкий Артем Владимирович, аспирант каф. АПВТ ХНУРЭ. Научные интересы: техническая диагностика. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 702-13-26.

Парфентий Александр Николаевич, аспирант каф. АПВТ ХНУРЭ. Научные интересы: техническая диагностика. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 702-13-26.

Чувило Олег Александрович, студент факультета Компьютерной инженерии и управления (каф. системотехники) ХНУРЭ. Научные интересы: анализ вредоносного кода. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 702-13-26.