СЕКЦІЯ 4. СИСТЕМИ БЕЗПЕКИ Й ЗАХИСТУ ІНФОРМАЦІЇ

УДК:004.7

ОРГАНИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ И САМОДИАГНОСТИКИ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

А.А.Косолапов, Д.В.Лоскутов, Н.А.Фастов
Днепропетровский национальный университет железнодорожного транспорта

В настоящее время информационные технологии и системы широко используются во всех сферах жизни общества. Они охватывают не только автоматизацию процессов сбора, хранения, обработки информации на крупных промышленных предприятиях, но сферу науки и образования. Современные информационные системы ВУЗов представляют собой крупные корпоративные сети из нескольких сотен компьютеров различных классов с выходом в глобальную сеть ИНТЕРНЕТ. Количество пользователей таких систем достигает нескольких десятков тысяч, а основным используемым ресурсом являются информационные базы данных. В этих условиях актуальной является многоаспектная проблема обеспечения информационной защиты корпоративных систем от вирусных атак различной природы.

Большую опасность для корпоративных сетей представляют вирусные атаки. Результатом таких атак может быть снижение производительности компьютеров, выход ПК из работоспособного состояния, потеря конфиденциальной информации и т.д. Решением проблемы может быть внедрение в корпоративную сеть комплексной системы антивирусной защиты на базе выбранного антивирусного программного обеспечения.

Был выполнен сравнительный анализ систем антивирусной защиты крупных корпоративных сетей. Источником

информации послужило издание "Virus Bulletin", которое с 1989 года занимается освещением вопросов, касающихся вирусов. На данный момент это издание занимает лидирующие позиции в своей области, ежегодно проводит конференции, на которых обсуждается информационная безопасность. Интересным является то, что с 1991 года журнал проводит независимое тестирование программных средств защиты. Результаты тестирования некоторых продуктов представлены ниже.

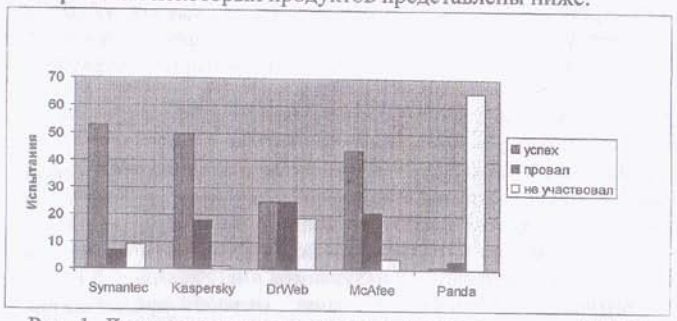

Рис. 1. Диаграмма прохождения антивирусами теста VB100

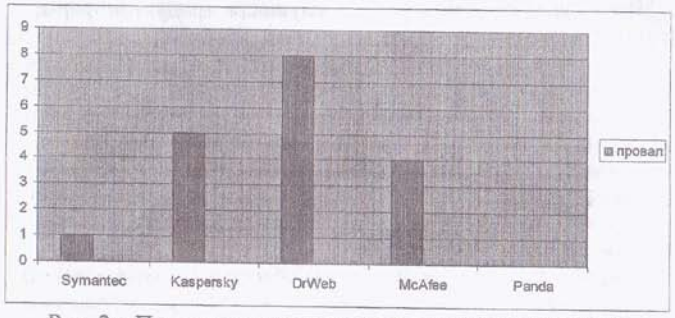

Рис. 2. «Провалы» антивирусов на VB100 за 2005-2010г

Тест VB100 основывается на так называемом WildList-списке. Этот список издается 1 раз в месяц антивирусными аналитиками бесплатно, указывая на наиболее

широкораспространенные угрозы в мире. Требования испытания VB100 следующие: обезвредить все вирусы из Wild-списка и при этом не вызвать ложных срабатываний (не назвать безвредный файл опасным). Если условия теста выполняются, то антивирусное ПО получает сертификат VB100.

Был выполнен анализ решения проблем обеспечения информационной защиты различными ВУЗами. Например, факультет права Гарвардского университета на своем сайте сообщает, что используемым антивирусным пакетом является продукция фирмы Symantec, даются рекомендации студентам и сотрудникам по установке продуктов, который возможно получить непосредственно с портала ВУЗа. Здесь же располагаются общие рекомендации по обеспечению информационной безопасности.

Американский университет для обеспечения антивирусной защиты учебных корпусов и общежитий используют продукты Symantec. Университет Род Айланда применяет средства McAfee. Ряд других заграничных академических учреждений используют продукты от Symantec и McAfee. ВУЗы постсоветского пространства чаще отдают предпочтение продуктам от Kaspersky, DrWeb, Panda и др.

Необходимо отметить ряд преимуществ продуктов фирмы Symantec по сравнению с другими антивирусами.

Во-первых, антивирусные продукты имеют одни из лучших показателей тестирования. Во-вторых, ПО широко используется в иностранных ВУЗах. В-третьих, специалисты в области антивирусной защиты утверждают, что использование программного обеспечения фирмы Symantec дает на порядок более высокий уровень защиты, нежели продукты других фирм. В-четвертых, продукт удобен в эксплуатации, дает широкие возможности в администрировании.

В связи с выше изложенным, для обеспечения комплексной системы антивирусной защиты в Днепропетровском национальном университете железнодорожного транспорта был выбран продукт Symantec Endpoint protection 11. В данное время система внедряется в корпоративную сеть университета. В лаборатории информационных технологий ДНУЖТ установлен

сервер управления корпоративным антивирусом. Он распределяет антивирусные сигнатуры, управляет политиками безопасности, следит за состоянием информационной безопасности отдельных узлов и корпоративной сети в целом. На данном этапе 150 компьютеров подключены к антивирусному серверу Symantec.

Однако применение только средств антивирусной защиты не обеспечивает полного и достоверного контроля состояния системы в условиях уязвимости центров диагностирования. Многомашинные сетевые конфигурации позволяют организовать распределённую диагностику систем с реконфигурацией топологии сети с учётом неработоспособных её узлов. Был выполнен анализ известных схем самодиагностики, отмечены возможности их применения.

Система диагностики представляет собой общую модель, состоящую из ряда устройств, в которых выполняются определенные нормально завершающиеся/приводящие к сбою тесты. Рассмотрим две схемы самодиагностики.

- диагностика для восстановления (ремонта);
- диагностика для допустимого уменьшения комплекта оборудования.

Задачи диагностики можно в большинстве случаев включить в термины, определяющие диагностическую информацию и диагностические приемники. Диагностическая информация- это информация, получаемая посредством диагностического процесса. Например, требуемой диагностической информацией могут быть: обнаружение одного отказавшего устройства, обнаружение всех отказавших устройств, или обнаружение некоторых устройств, связанных с рядом неотказавших устройств.

Диагностические приемники- это ряд устройств в системе, которые могут получать эту информацию. С помощью специальных различных комбинаций диагностической информации и диагностических приемников, можно определить широкое разнообразие задач самодиагностики.

Рассмотрим 2 возможных цели диагностики:

1. Ремонт(восстановление): система периодически

подвергается диагностике так, что отказавшие устройства могут быть восстановлены, и таким образом сохраняется работоспособность системы в полном объеме. Восстановление может быть ручным, или в форме резерва, который включается в систему к оставшимся работоспособным устройствам.

2. Допустимое уменьшение комплекта (оборудования): первоначально система имеет избыток объема оборудования, и по мере выхода из троя устройств система продолжает функционировать, распределяя задачи между оставшимися работоспособными устройствами. Диагностика здесь необходима в порядке определения той части системы, которая еще функционирует.

Рассмотрим выборы диагностической информации и диагностических приемников в каждом из этих случаев.

В случае диагностики для восстановления предполагается, что восстановление не происходит один раз, цикл диагностика\восстановление может повторяться до тех пор, пока не будет работоспособной вся система. Таким образом, нет необходимости обнаруживать все ошибки за один цикл диагностики. Достаточно определения одного отказавшего устройства. Система, проводящая диагностику для восстановления, может содержать один или несколько диагностических «контроллеров», которые выполняют восстановление или замену. Контроллер может осуществлять реконфигурацию устройства управления, способного автоматически переключаться на резерв или осуществлять восстановление с помощью человека.

В случае диагностики для допустимого уменьшения комплекта (оборудования) задача не столь длинная для точного определения отказавших устройств, сколько более верная при определении некоторого ряда работоспособных устройств из числа оставшихся, способных функционировать. Диагностическими приемниками здесь выступают те устройства, которые служат для отсоединения отказавших или подозреваемых в отказе устройств. Этот случай не похож на случай «диагностики для восстановления», здесь не предполагается наличие специальных контроллеров, которые

способны к широкосистемной реконфигурации. Скорее есть необходимость отсоединения локальных отказавших устройств, которые распределены среди «интеллектуальных» устройств системы (названы тестерами). Тестеры выполняют диагностику, затем отсоединяют ту из любых частей системы, которая не может быть проверена из-за отказа. Отсоединение может проводиться путем отключения или выключения устройств, путем электрического разрыва каналов передачи или путем блокировки отказа или подозрения на отказ.

Вопросы самодиагностики освящены в статьях Р. Неира, Г. Мейера, А. Макензи и др. В них предполагаются математические допущения, используя которые можно получить алгоритмы самодиагностики: алгоритм первичной загрузки, алгоритм обнаружения с помощью прямого метода, алгоритм для допустимого уменьшения комплекта оборудования и др. Проведенный анализ показал, что требуются дальнейшие исследования и разработка методов самодиагностики, например, методов инициирования диагностического тестирования. Механизмы распределенного контроля функционирования и диагностики систем позволят обеспечить более полный и достоверный контроль состояния системы в условиях уязвимости диагностируемых узлов.

Литература:

1. Craig S. Holt, James E. Smith. "Self-Diagnosis in distributed systems", IEEE Transactions on Computers. Vol.34, pp.19-32, Jan. 1985.