**Оптимальная антивирусная защита информации**

Асп. Сорокин С.В. Кафедра автоматизации обработки информации. Северо-Кавказский государственный технологический университет

Построены модели функционирования антивирусной защиты информации и процесса проникновения и размножения вирусной инфекции в вычислительной системе. сформирована задача определения режима оптимального функционирования антивирусной защиты информации. предложен и сформирован подход раздельной защиты информации, позволяющий уменьшить использование ресурсов вычислительной системы, выделяемых на поддержание защиты.

Для минимизации потерь информации на файловых серверах, повышения надежности работы вычислительной системы необходимо периодически проводить тестирование хранящихся данных антивирусным программным обеспечением (авпо).далее будем исходить из того, что:

вся хранимая информация находится на жестком диске;

последствия проникновения и действие вирусов обратимы.

Процессорное время сервера распределяется по следующим направлениям: системные затраты времени; обработка запросов пользователей; тестирование хранящейся информации на наличие вирусов; восстановление информации, разрушенной вирусами. целью администратора вычислительной сети является такая организация работы сервера, при которой максимизировалось бы время, выделенное для обработки запросов пользователей, для чего необходимо минимизировать затраты процессорного времени сервера на “самообслуживание”, т.е. на тестирование и восстановление информации. иными словами, необходимо определить оптимальный режим работы авпо.

Используются следующие обозначения:

- срок обеспечения защиты;



- время тестирования информации;



- время на восстановление информации;



- время работы авпо (т = + );



Δt - интервал времени между двумя тестированиями, [0, ts];

-квант времени;



v- объем тестируемой памяти;

- количество тестируемых файлов;



ϕ-интенсивность размножения вирусов;

μ- интенсивность гибели вирусов;

η- интенсивность проникновения вирусов в систему;

λ- скорость восстановления информации;

-время подготовки к тестированию одного файла;



-время тестирования единицы информации.



допущения:

Будем исходить из того, что распространение инфекции происходит в среде с постоянными характеристиками (объем озу, быстродействие процессора, накопителей, системной шины).

Скорость восстановления и тестирования информации постоянна и зависит от типа авпо.

Используемые антивирусные средства восстанавливают зараженные файлы, а если восстановление невозможно, то удаляют их из памяти, т.е. после тестирования вирусы в системе отсутствуют.

Содержательная постановка задачи. исходя из того что вся информация хранится в эвм на жестком диске и последствия проникновения вирусов обратимы (разрушенная информация может быть восстановлена, например, путем удаления из нее зловредного кода либо полного копирования с зеркального диска или архива), получаем распределение процессорного времени: системные затраты времени; решение задач пользователей; тестирование информации авпо; восстановление информации авпо.

Следовательно, целью оптимизации является нахождение оптимальной частоты тестирования, учитывая как характеристики программного обеспечения (авпо), так и характеристики аппаратуры (сервера, вычислительной сети, топология сети). а целью работы вс является максимизация времени, выделяемого на решение задач пользователей, что ведет к минимизации времени работы авпо.

Формальная постановка задачи. очевидно, что рост частоты тестирования ведет к своевременному обнаружению и уничтожению вирусов и снижению времени восстановления разрушенной информации, но увеличивает суммарное время тестирования информации.

Таким образом, инструментом оптимизации является промежуток времени между двумя тестированиями . время тестирования определяется из выражения



. (1)



Величины f и v определяются, используя стандартные функции системы. величины ,и являются характеристиками авпо и определяются во время установки защиты.



Как известно, вирусная инфекция не только разрушает информацию, но размножается и гибнет (дезактивируется). процесс размножения и гибели вирусов может быть представлен моделью (2) изменения объема совокупности, члены которой могут погибать (или исчезать любым другим способом) [1]:

, (2)



где - количество вирусов в системе при .



Проникновение вирусов в систему можно рассматривать как биноминальное распределение [1]. пусть - число вирусов, поступивших в систему за время с интенсивностью :



. (3)



при число вирусов, находящихся в системе к моменту времени t, определяется выражением



(4)



или

. (5)



из допущения (3) , (5) следует:

. (6)



Накапливая статистические данные зависимости , и пользуясь методом наименьших квадратов, величины можно определить, минимизируя среднеквадратическое отклонение найденной аналитической зависимости от накопленных статистических данных:



, (7)



где g – среднеквадратическое отклонение; n - количество накопленных данных;и - статистические данные.



Вследствие трансцендентности функций (7) воспользуемся методом поиска минимума функций нескольких переменных [2].

Определяя величины , время восстановления информации запишется в виде:



. (8)

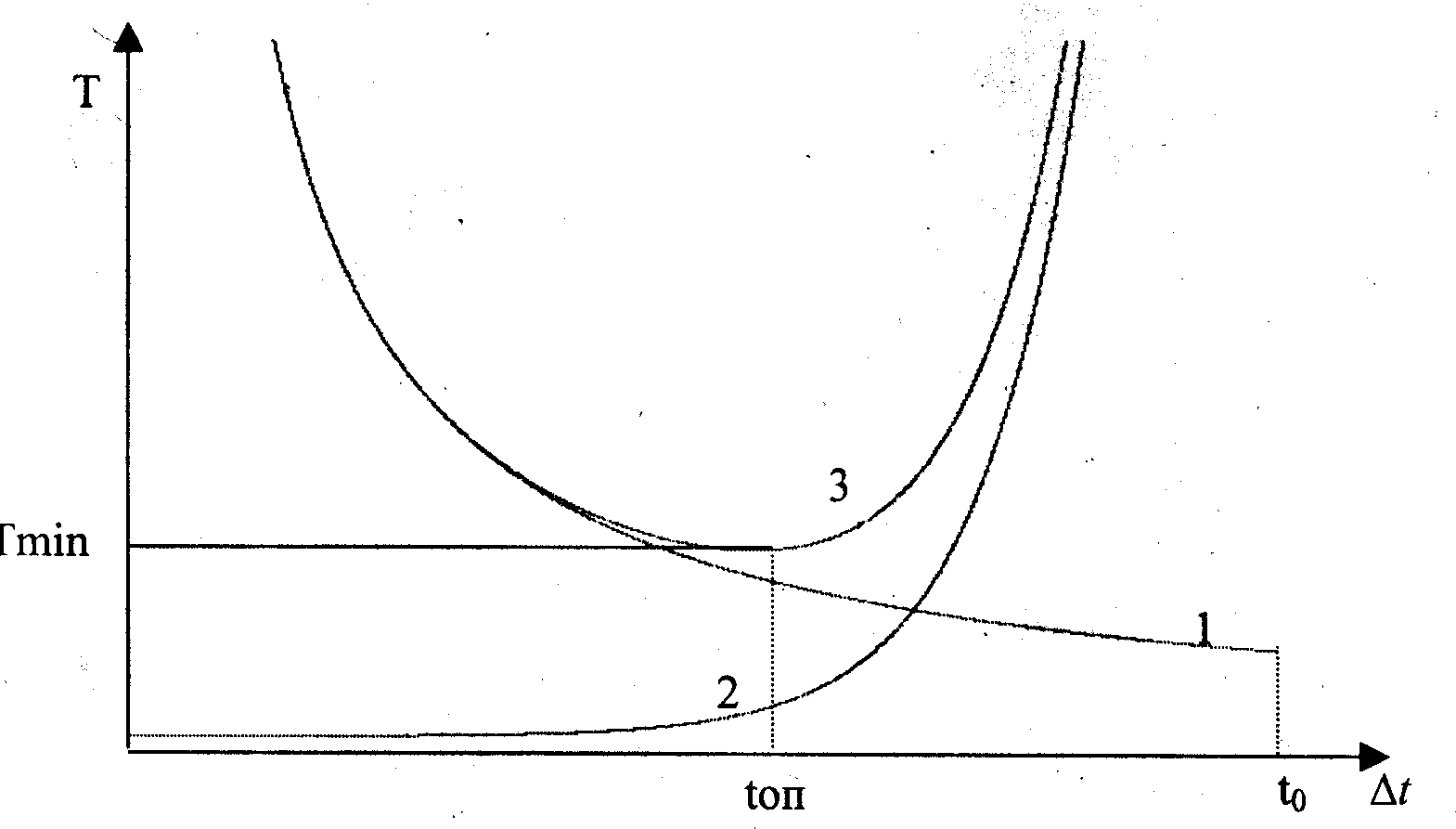


Суммируя (1) и (8), получаем время работы авпо:

. (9)



Задача поиска оптимального режима работы авпо сводится к минимизации правой части (9), решением является оптимальный интервал между запусками авпо tопт при времени работы авпо, равном тmin (рисунок).



зависимость времени работы авпо от времени между тестированиями. время тестирования (1), восстановления (2), работы авпо (3).

1



t0

Выражение (9) является трансцендентным, и поиск минимального его значения осуществляется при помощи численных методов поиска минимума функций одной переменной [2].

Применение раздельной защиты. как известно, различные типы вирусов инфицируют различные типы информации. ввиду того что информация в вычислительных системах разнородна и имеет разные характеристики (частота использования, подверженность вирусным атакам и т.д.), имеет смысл осуществлять раздельное сканирование Различных типов информации и определять параметры защиты для каждого типа информации отдельно, избегая при этом избыточного тестирования файлов, не представляющих угрозу. время, затраченное на поддержание антивирусной защиты s типов информации, имеет вид:

, (10)



где-характеристики вычислительной системы для с-ого типа информации.



Нахождение аналитического решения системы (10) сводится к нахождению оптимального режима защиты отдельно для каждого типа информации.

Заключение. предлагаемый подход эффективного использования авпо, учитывая характеристики вычислительной системы и внешнего воздействия на систему защиты, приводит к увеличению серверного времени, затрачиваемого на решение задач пользователей. применение индивидуального подхода для каждого типа информации позволяет определить глобально оптимальный режим работы системы антивирусной защиты, а это обеспечивает высокий уровень защиты без наращивания мощностей вычислительной системы, избегая избыточного тестирования. достоинствами данного подхода является инвариантность относительно используемых авпо, типов информации, топологии сети и платформы сервера. рассмотренный подход наиболее эффективен при использовании на корпоративных файлах, web-серверах.

**Список литературы**

1. Феллер В. Введение в теорию вероятностей и ее приложения. м.: мир, 1982.

2. Банди Б. Методы оптимизации. вводный курс. м.: радио и связь, 1998.