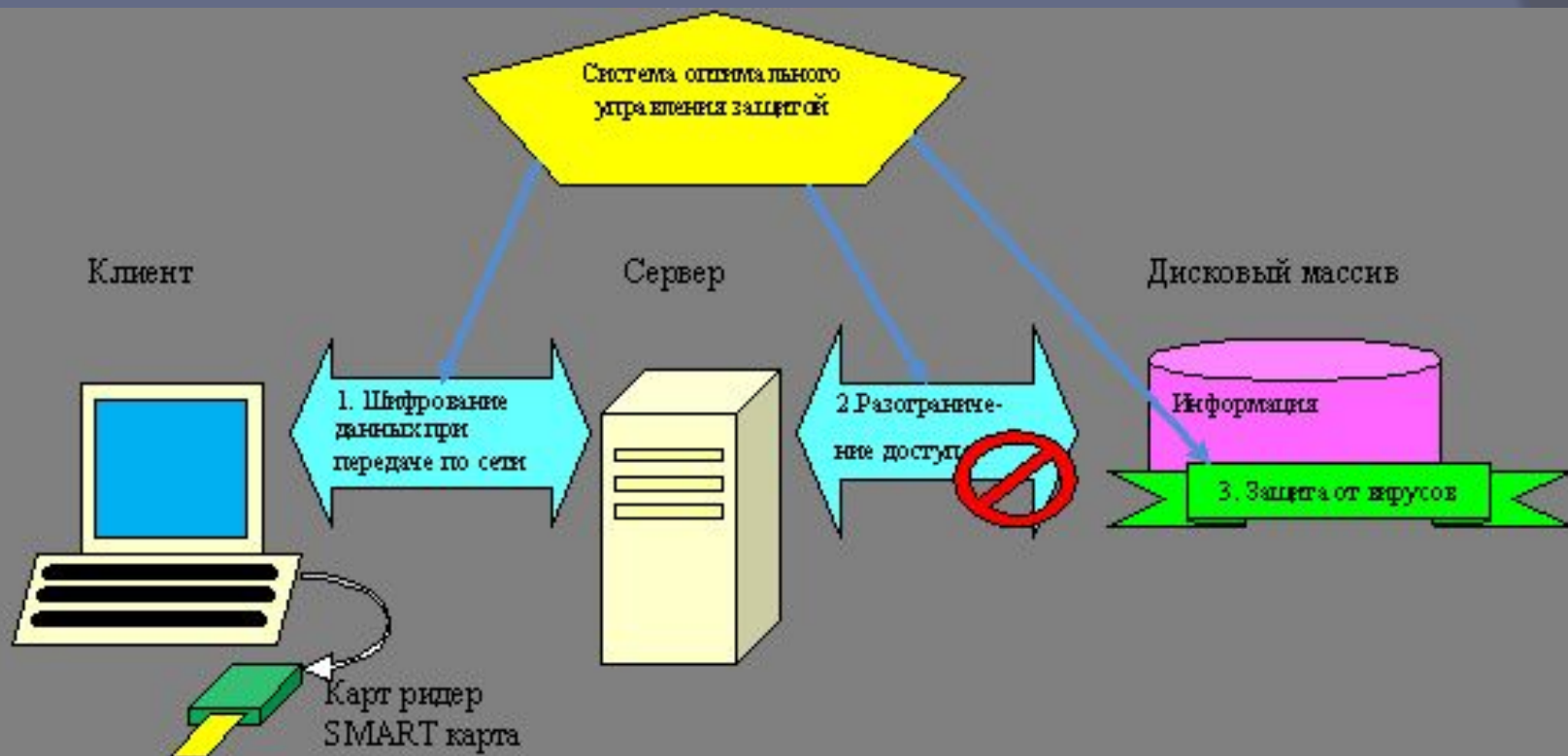


# ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ

Направление: Автоматизированные системы  
обработки информации и управления

Лекция 3 Борьба с несанкционированным доступом  
и вирусами

# Три ступени защиты информации



# Уровни и средства антивирусной защиты

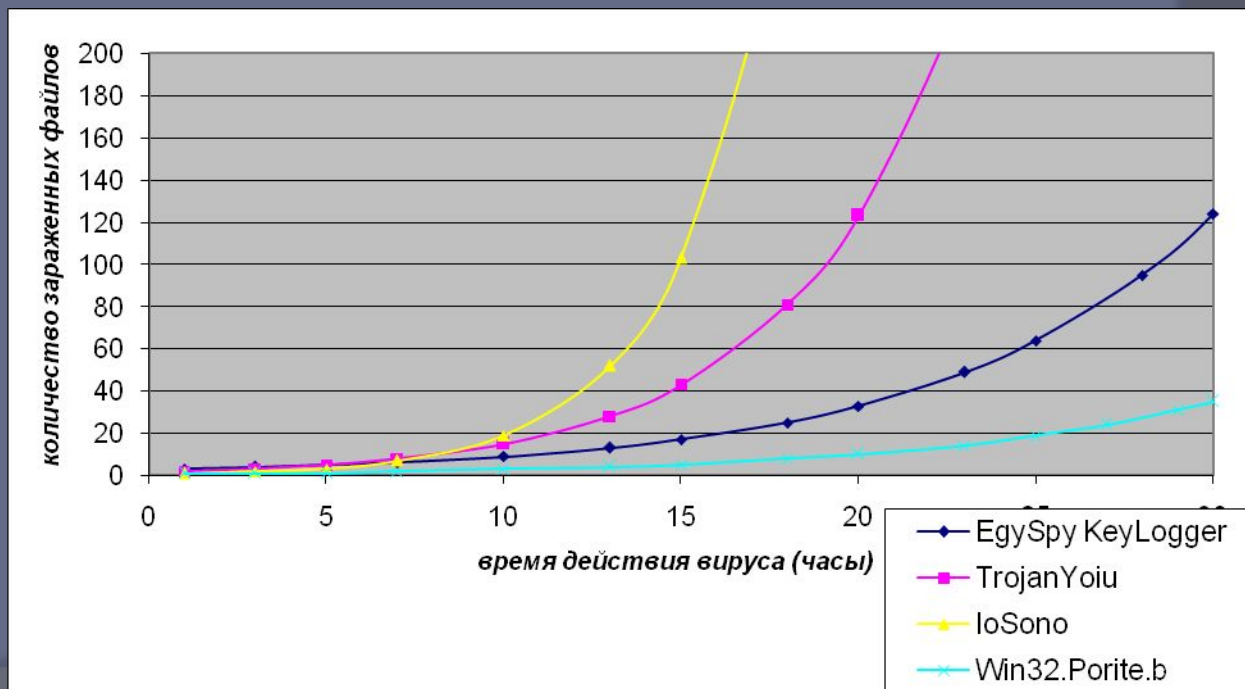


# Результаты имитационного моделирования

- Экспериментальный анализ поведения поражающих программ состоит из двух частей.
- Первый этап экспериментов проводился для нескольких видов вредоносных программ при их единичном, изолированном воздействии на операционную систему.
- Вторым этапом экспериментов выполнялся для нескольких видов различных вредоносных программ при их совместном, комбинированном воздействии на систему.

# Анализ одиночного воздействия определенного вируса

- Обобщив результаты проведенных на первой этапе эксперимента исследований, можно сказать, что общим для всех вирусов является экспоненциальный характер роста числа зараженных файлов, имеющих на виртуальном жестком диске, с течением времени воздействия (активности) той или иной вредоносной программы.



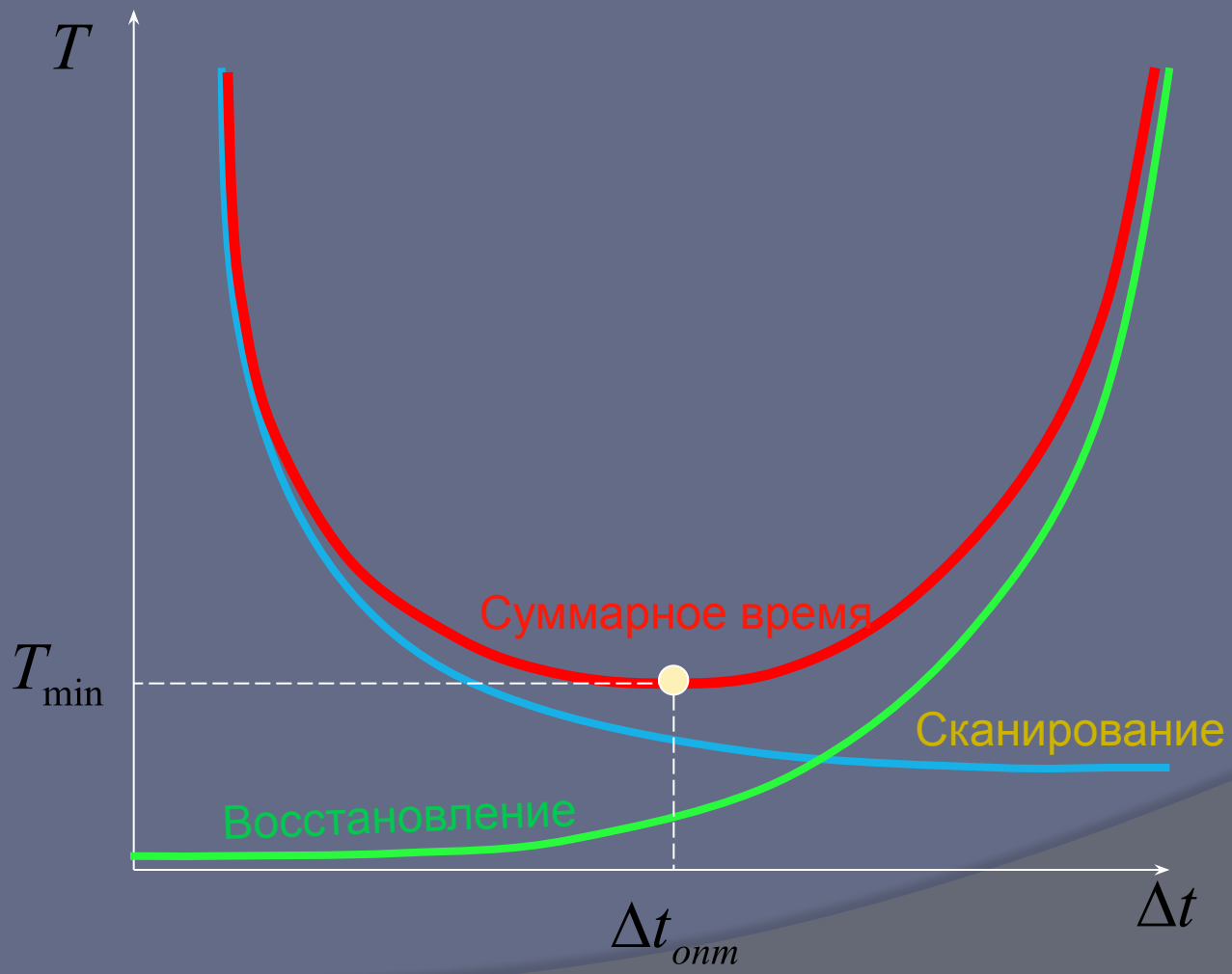
# Эффективная борьба с вирусами

- Работа любого антивирусного сканера определяется тремя функциями:
  1. Сканирование памяти компьютера на предмет поиска вирусов и запорченных данных.
  2. Блокада либо уничтожение вирусов.
  3. Восстановление запорченной информации.

# Количественные зависимости

- Затраты времени  $T_1$  на сканирование памяти компьютера прямо пропорциональны частоте запуска сканера  $f$ :  $T_1 = a \cdot f$ , где «а» – коэффициент.
- Затраты времени  $T_2$  на восстановление запорченных файлов в первом приближении обратно пропорциональны частоте запуска сканера:  $T_2 = b/f$ .

# Зависимость объема потребленных ресурсов (время $T$ ) от интервала времени между запусками транзитного сканера $\Delta t$

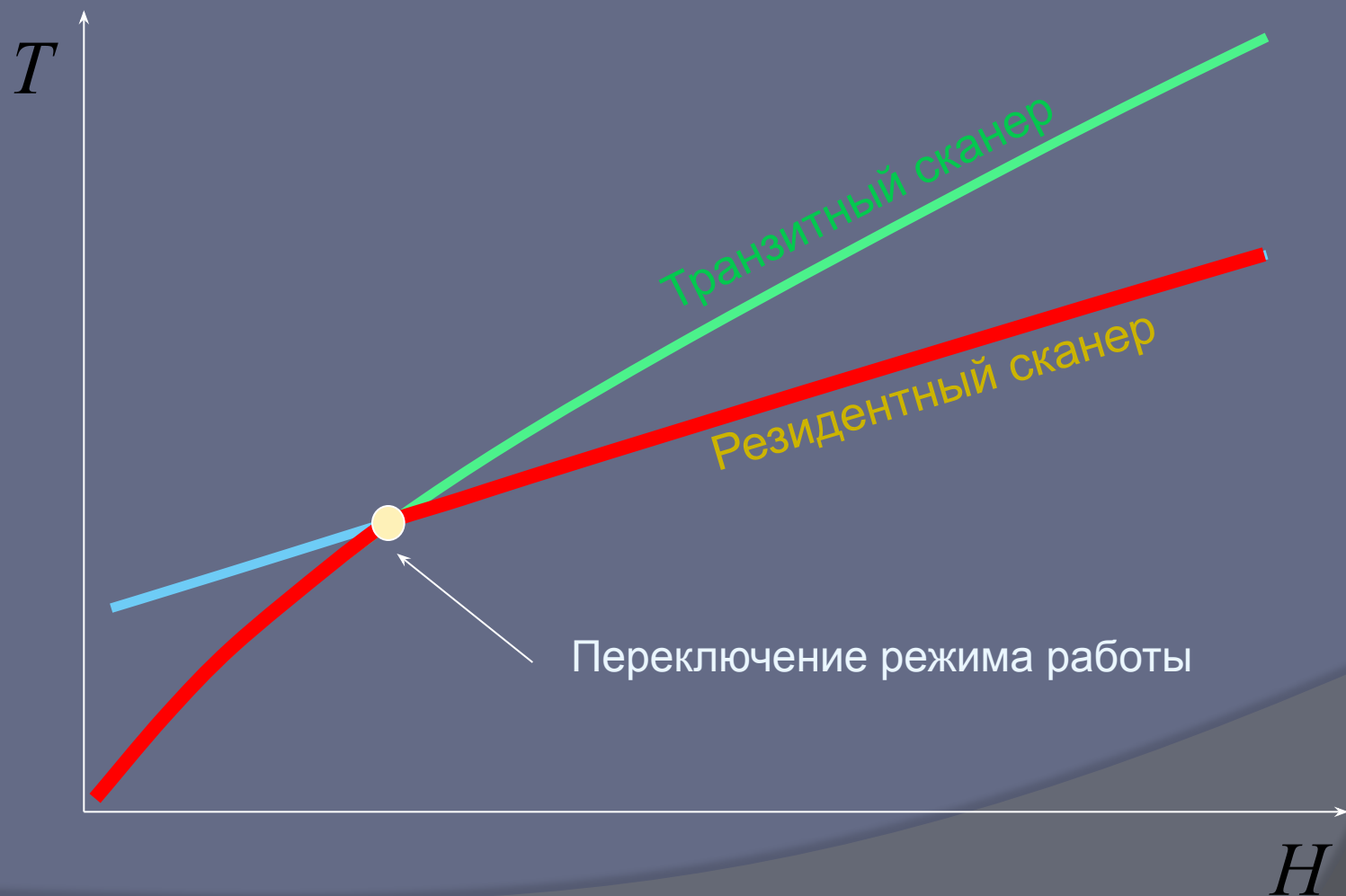




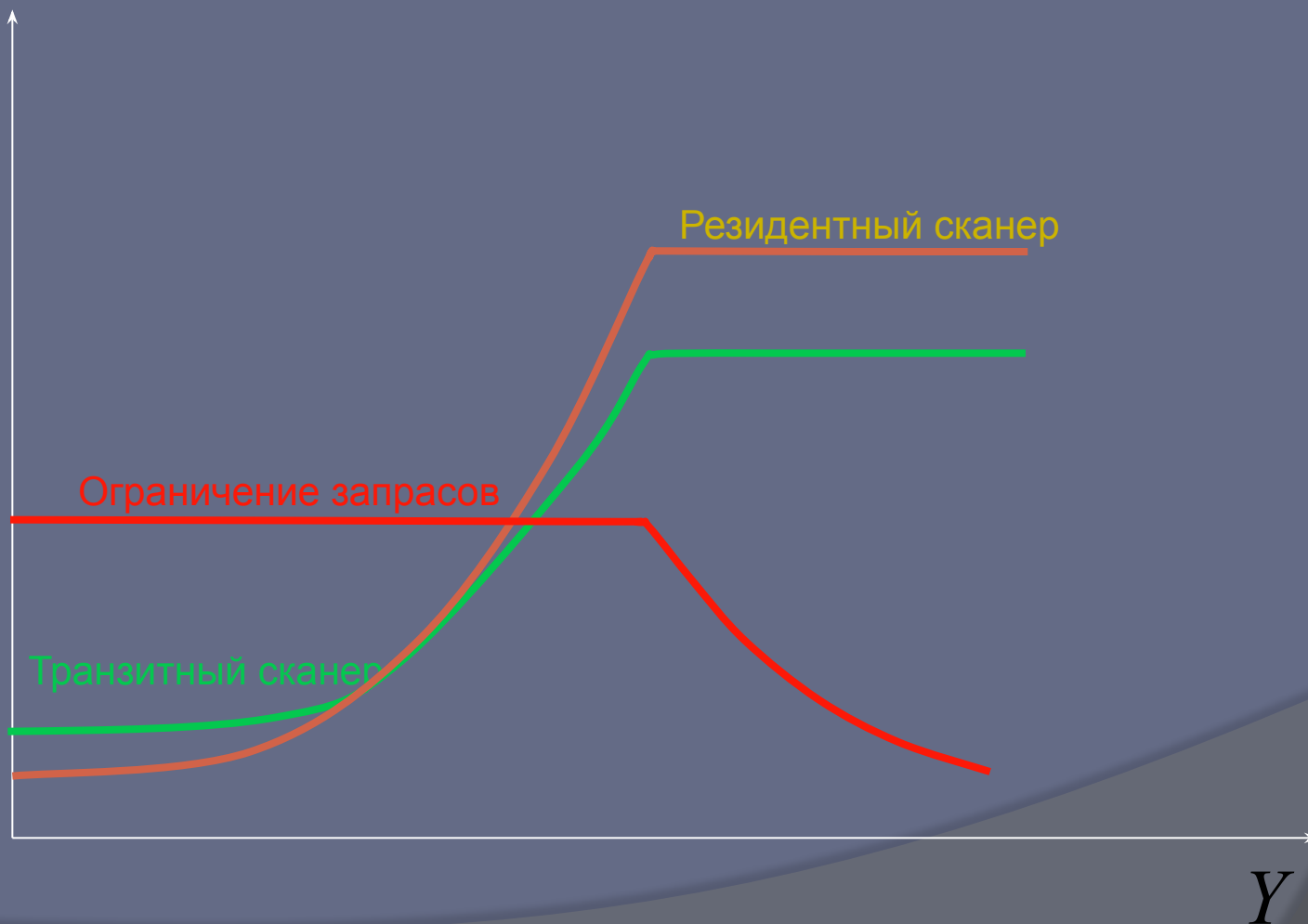
## Задачи, решаемые пакетом *“Smart Protection”*:

1. Определение характеристик системы:
  - интенсивность проникновения вирусов в систему
  - интенсивность обработки файлов в системе (запуск на выполнение)
2. Определение количества зараженных файлов в системе на момент следующего сканирования.
3. Определение интервала между сканированиями, минимизирующего потребление ресурсов ЭВМ.
4. Выбор типа используемого сканера (транзитный или резидентный), минимизирующего потребление ресурсов.
5. Защита от перегрузок.

# Зависимость потребления ресурсов сервера $T$ от интенсивности вирусных атак $H$



# Зависимость потребления ресурсов и ограничения трафика пакетом “Smart Protection” от интенсивности работы пользователей $Y$ в режиме перегрузки



# Пример 2

- Содержательная постановка задачи: требуется определить оптимальную частоту запуска антивирусного сканера, минимизирующую затраты на борьбу с вирусами.
- Формальная постановка задачи:  
$$T = T_1 + T_2 \rightarrow \min,$$
или:  $a \cdot f + b/f \rightarrow \min.$

# Экспериментальные данные

- Экспериментальные данные:

| F (Гц) | T (сек) |
|--------|---------|
| 1      | 27      |
| 3      | 11      |
| 5      | 3       |
| 8      | 6       |
| 10     | 18      |

- Предлагаемое решение:  $f = 5$ ;  $T = 3$ .

# Алгоритм поиска оптимальной частоты запуска сканера

Шаг 1. Ввод экспериментальных данных.

Шаг 2. Поиск аналитической зависимости  $T(f)$  методом наименьших квадратов.

Шаг 3. Численное решение уравнения  $dT/df = 0$ .

Шаг 4. Конец алгоритма.

# Решение примера 2

| f  | T  |
|----|----|
| 1  | 27 |
| 3  | 11 |
| 5  | 3  |
| 8  | 6  |
| 10 | 18 |

Уравнение  $T(f)$  имеет вид:

$$T = f^2 - 12f + 38.$$

Оптимальное значение  $f$  равно шести.

Минимальные затраты времени на антивирусную защиту равны двум.

Величина выигрыша  $\eta = 1,5$ .

# Самостоятельно

- Пользуясь описанным выше алгоритмом, определить оптимальную частоту запуска антивирусного сканера и выигрыш, если экспериментальные данные представлены таблицей:

| f  | T    |
|----|------|
| 1  | 15   |
| 3  | 13   |
| 5  | 17,4 |
| 12 | 37   |



# Аналитический вид зависимости $T(f)$

- ◎  $T_1 = 3f.$
- ◎  $T_2 = 12/f$
- ◎  $T = T_1 + T_2.$