МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»
ФГБОУ ВПО
ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ

Направление: 09.04.02 Информационные системы и технологии
Кафедра: Информационных технологий моделирования и управления

# Разработка подсистемы управления доступом инфраструктуры безопасности распределительных информационно вычислительных систем

*Автор: студент гр. Ум-153 Ширинкин Н.В.,*
*Руководитель: профессор, д.т.н. Скрыпников А.В.*

**Воронеж 2017**

# Цели и задачи

**Цель**: оценка и регулирование риска возникающего в ходе функционирования сервера базы данных банковской сети.

***Задачи:***

1. Выявление закономерностей, которым подчиняются исследуемые процессы реализации атак на серверы баз данных банковской сети.
2. Построение математической модели атак, реализуемых на сервера базы данных банковской сети.
3. Оценка риска успешной реализации атаки на сервер базы данных банковской сети; нахождение зависимости изменения параметров риска с течением времени, создание методики поиска эффективного решения по регулированию риска, нахождения области допустимого риска для атакуемого сервера базы данных. Создание алгоритма поиска оптимального решения по регулированию риска
4. Оценка экономических показателей эффективности разработанных алгоритмов.

# Аргументация метода моделирования

Чтобы воспользоваться механизмом моделирования с помощью сетей Петри-Маркова необходимо доказать три свойства атаки:

- стационарность;

То есть, вероятность реализации атаки постоянна.

- ординарность;

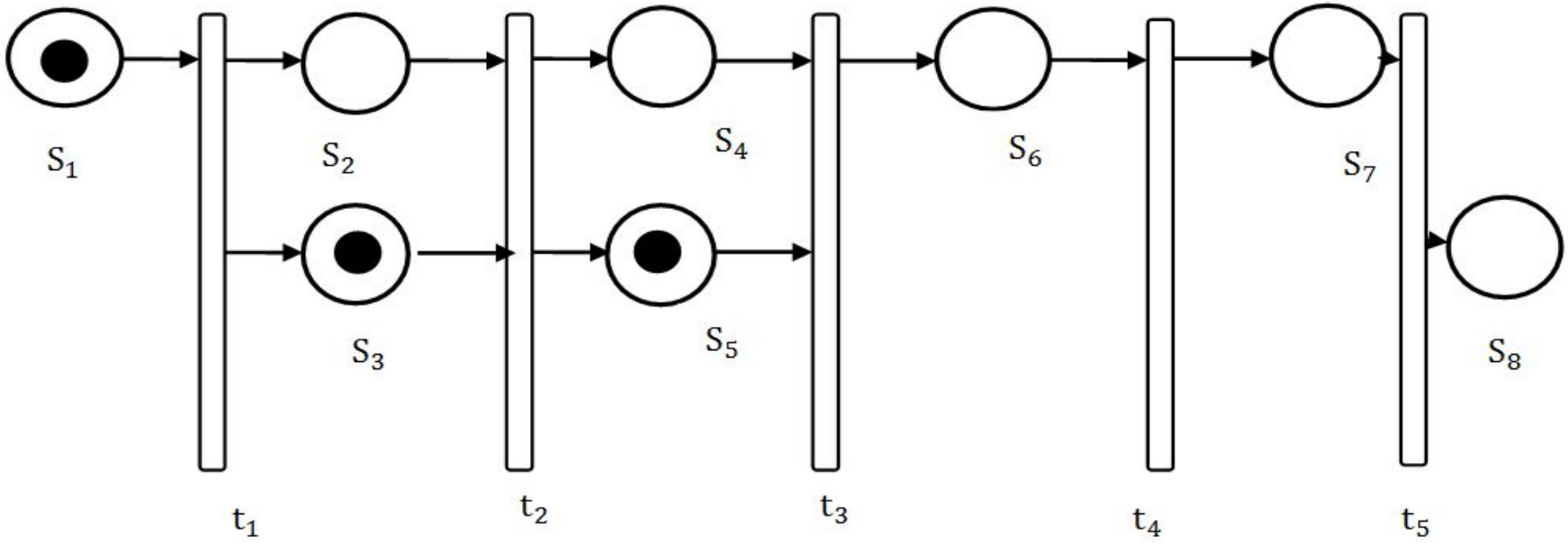
В единицу времени t приходит только одна атака.

- отсутствие последействия.

Вероятность не зависит от момента совершения предыдущих событий (данный факт и будет допущением в данном исследовании).

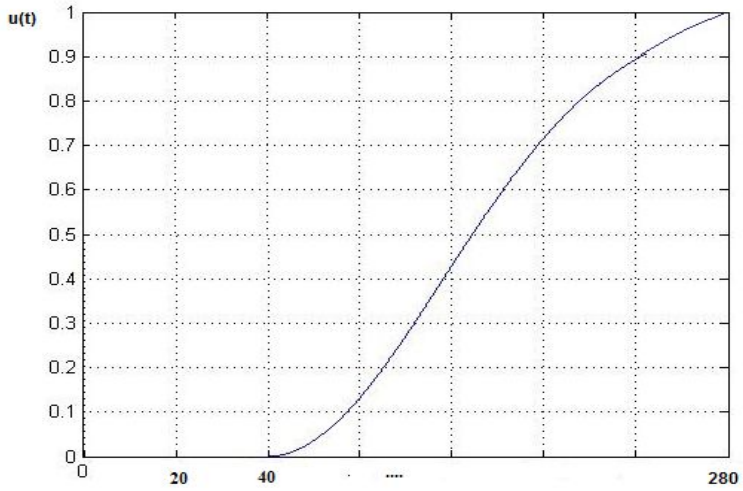
# Моделирование процесса атаки

Вид сети Петри-Маркова для общего вида атаки на  сервер



# Функция ущерба

$$u(t) = \begin{cases} 1 - e^{-\frac{\omega \cdot P \cdot (t - t_0)}{\rho}}, & t < 280 \\ \frac{280}{pt}, & x \geq 300 \end{cases}$$




1

где:

$\rho$ – количество полезной информации полученной злоумышленником;

$\omega$ – интенсивность обращений к СУБД банковского сервера;

$t_0$ - время начала атаки;

P - общее число информации, полученное злоумышленником;

$t$ - время реализации атаки.

2

.

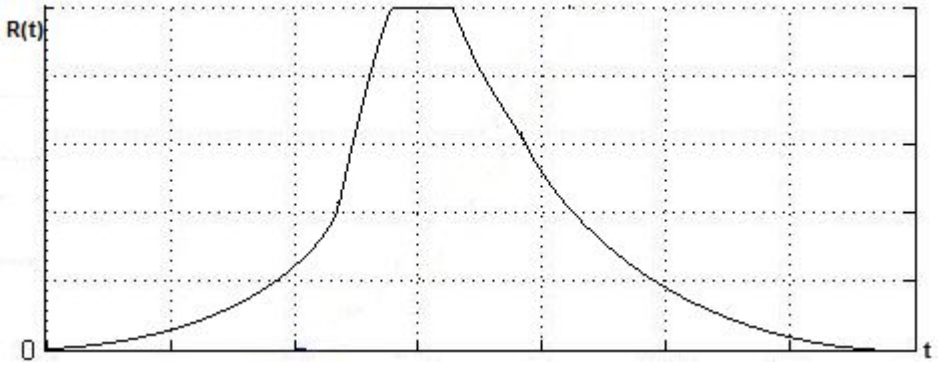
$p$ – интенсивность принятия продуктивных решений;

$t$ - время ответных действий.

# Риск и шанс

$$Ch = e^{-\frac{(t-\tau_a)}{\tau}} - e^{-\left(\frac{\omega \cdot P \cdot t}{\rho} + \frac{(t-\tau_a)}{\tau}\right)},$$

$$Risk(t) = \frac{e^{-\frac{(t_0)}{\tau}}}{\tau} \cdot \left(1 - e^{-\frac{\omega \cdot P \cdot (t-t_0)}{\rho}}\right)$$




Графическое представление функции риска

где:
$\rho$ – количество полезной информации полученной злоумышленником;
$\omega$ – интенсивность обращений к СУБД банковского сервера;
$t_0$ - время начала атаки;
P - общее число информации, полученное злоумышленником;

# Полезность и живучесть

$$U(t) = 1 - e^{-\frac{\omega \cdot P \cdot t}{\rho}}$$

$$L = \frac{Ch}{Risk} = \tau \cdot \frac{e^{-\left(\frac{\omega \cdot P \cdot t}{\rho} + \frac{(t-\tau_a)}{\tau}\right)}}{\left(1 - e^{-\frac{\omega \cdot P \cdot (t-t_0)}{\rho}}\right)}$$

где:

$\rho$ – количество полезной информации полученной злоумышленником;

$\omega$ – интенсивность обращений к СУБД банковского сервера;

$t_0$ - время начала атаки;

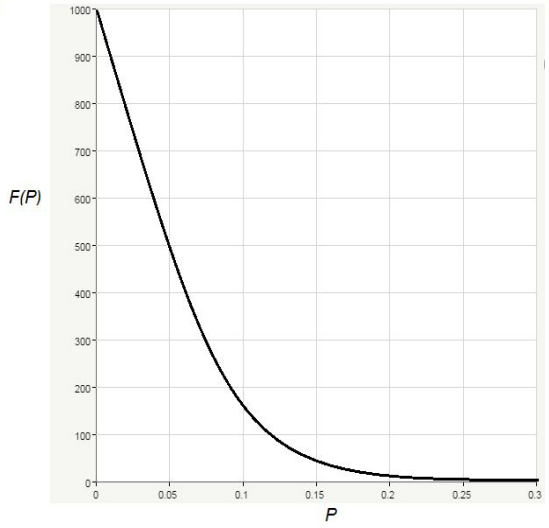
P - общее число информации, полученное

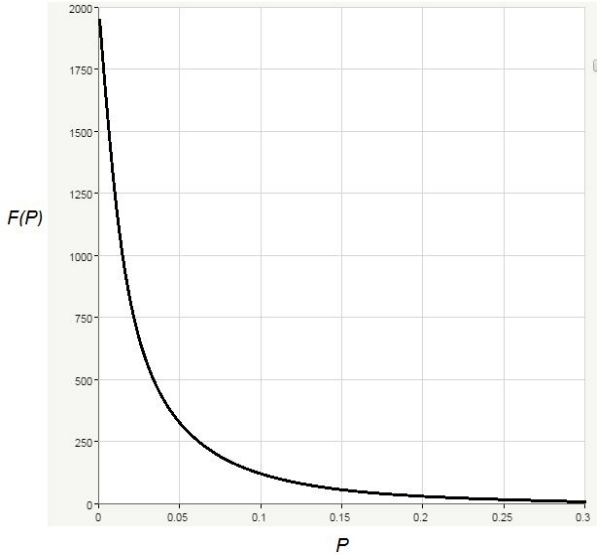
# Аналитические выражения для расчетов параметров риска

| Параметр риска | Соответствующее аналитическое выражение |
|---|---|
| Математическое ожидание | $\Delta t e^{\frac{\tau_a}{\tau}} \cdot \frac{\left(\tau \cdot \frac{\omega \cdot P}{\rho} \cdot e^{-\frac{\omega \cdot P}{\rho} \cdot t_0} + \tau \cdot e^{-\frac{\omega \cdot P}{\rho} \cdot t_0}\right)}{\left(\tau \cdot \frac{\omega \cdot P}{\rho} + 1\right)}$ |
| Интегральный риск | $\Delta t e^{\frac{\tau_a}{\tau}} \cdot \frac{\left(\tau \cdot \frac{\omega \cdot P}{\rho} \cdot e^{-\frac{\omega \cdot P}{\rho} \cdot t_0} + \tau \cdot e^{-\frac{\omega \cdot P}{\rho} \cdot t_0}\right)}{\left(\tau \cdot \frac{\omega \cdot P}{\rho} + 1\right)}$ |
| Среднее значение ущерба | $M^* = 2\tau$ |
| Среднеквадратическое отклонение | $\sigma^* = 2\tau$ |
| Мода риска | $t_0 - \frac{ln\left(\frac{\tau \cdot \frac{\omega \cdot P}{\rho} - 1}{\tau \cdot \frac{\omega \cdot P}{\rho}}\right) \cdot \rho}{\omega \cdot P}$ |
| Пик риска | $\frac{e^{-\frac{\left(t_0 - \frac{ln\left(\frac{\tau\frac{\omega \cdot P}{\rho} - 1}{\tau\frac{\omega \cdot P}{\rho}}\right)}{\frac{\omega \cdot P}{\rho}} - \tau_a\right)}{\tau}}}{\tau} \cdot \left(1 - e^{ln\left(\frac{\tau\frac{\omega \cdot P}{\rho} - 1}{\tau\frac{\omega \cdot P}{\rho}}\right)}\right)(\Delta t)$ |

# Расчет и анализ матрицы компонентов чувствительности риска

$$S^{Risk} = \begin{pmatrix} S_{\tau}^{Risk\_ln} \\ S_{\tau_a}^{Risk\_ln} \\ S_{\rho}^{Risk\_ln} \\ S_{\omega}^{Risk\_ln} \\ S_{t_0}^{Risk\_ln} \\ S_{P}^{Risk\_ln} \end{pmatrix} = \begin{pmatrix} -\frac{t-\tau_a}{\tau} \\ \frac{\tau_a}{\tau} \\ \frac{\tau^2 \cdot e^{-\frac{\omega \cdot P \cdot (t-t_0)}{\rho}}}{\rho \cdot \left(1 - e^{-\frac{\omega \cdot P \cdot (t-t_0)}{\rho}}\right)} \\ \frac{e^{-\frac{\omega \cdot P \cdot (t-t_0)}{\rho}}}{\omega \left(1 - e^{-\frac{\omega \cdot P \cdot (t-t_0)}{\rho}}\right)} \\ \frac{e^{-\frac{\omega \cdot P \cdot (t-t_0)}{\rho}}}{t_0 - t_0 \cdot e^{-\frac{\omega \cdot P \cdot (t-t_0)}{\rho}})} \\ \frac{e^{-\frac{\omega \cdot P \cdot (t-t_0)}{\rho}}}{P\left(1 - e^{-\frac{\omega \cdot P \cdot (t-t_0)}{\rho}}\right)} \end{pmatrix}$$



# Аналитическая оценка

где:

$\rho$ – количество полезной информации полученной злоумышленником;

$\omega$ – интенсивность обращений к СУБД банковского сервера;

$t_0$ - время начала атаки;

P - общее число информации, полученное злоумышленником;

$t$ - время реализации атаки.

# Выводы

- Описана схема реализации атак на СУБД банковских систем с помощью сетей Петри-Маркова
- Разработана модель защиты от атаки на СУБД банковских систем, выявлена закономерность распределения ущерба согласно модели атаки
- Произведена оценка риска и его компонентов
- Проведена оценка чувствительности рисков
- Выявлены меры по регулированию риска