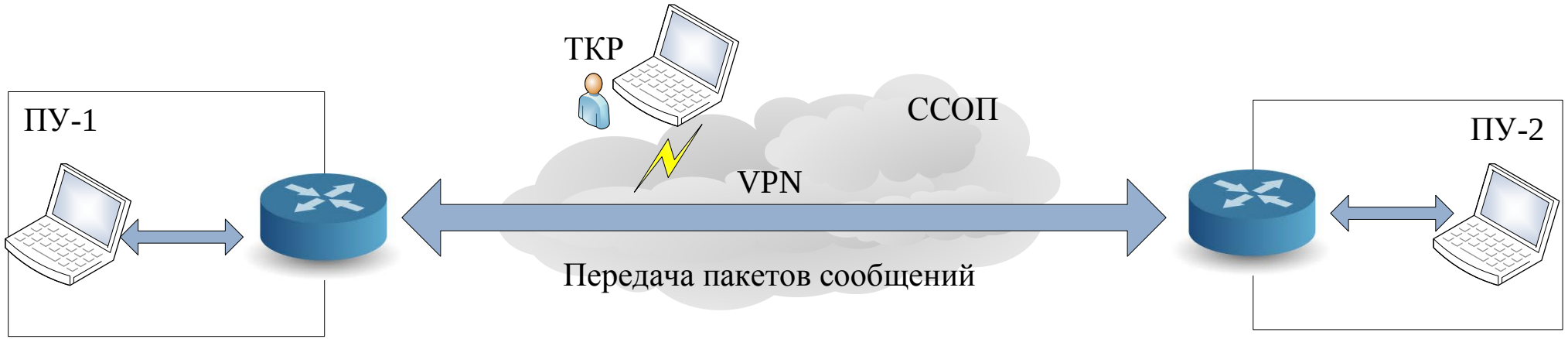
Краснодарское высшее военное училище
имени генерала армии С.М. Штеменко

Доклад на тему :

«Модель верификации результативности маскирования структуры информационных систем»

Выполнил: Каплин Максим Андреевич



ДЕМАСКИРУЮЩИЕ ПРИЗНАКИ

- Идентификаторы (логические и физические адреса)
- Наличие инф. потоков в КС, идентификаторы корреспондирующих узлов
- Объемы трафика между узлами СС (время суток, оперативных фон)
- Поля заголовков и поле данных пакетов сообщений
- Информационный обмен с другими узлами, управляющий трафик, функции узла, место в структуре

ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ

ИНВАРИАНТЫ СОСТАВА ИС

- Множество узлов
- Схема инф. связей
- Интенсивность инф. обмена
- Протоколы взаимодействия
- Уровни иерархии (ранги узлов) ИС

ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ

МОДЕЛИ

- Модель состава ИС ВН
- Модель структуры ИС ВН
- Модель информационного обмена ИС ВН
- Оперативная модель ИС ВН

ОБОБЩЕНИЕ И АНАЛИЗ

- Множество узлов
  - Множество оборудования
    - Множество ПО
- Схема инф. связей
  - Структура ИС ВН
    - Топология ИС ВН
- Интенсивность инф. обмена
  - Протоколы взаимодействия
  - Функции УС
    - Уровни иерархии

Дано:

S - Клиент-серверная ИС
C - Множество входных параметров ИС
A - Запросы СУ
B - Воздействие ТКР
Z - Множество внутренних параметров ИС
P_i - Множество выходных параметров модели, значения финальных вероятностей состояния системы S
I - множество параметров условий функционирования
Q - Показатель эффективности маскирования логической структуры ИС
μ - Модель клиент серверной ИС S

Найти: закономерность изменения множества P_i выходных параметров модели верификации результативности маскирования логической структуры ИС и множества Q показателей эффективности маскирования логической структуры ИС от множества C значений входных параметров, множества Z значений внутренних параметров, множества I значений параметров условий функционирования. На значения параметров множеств C, P_i, Z, I наложены условия их допустимости

Формализованная постановка задачи на моделирование верификации результативности маскирования логической структуры ИС:

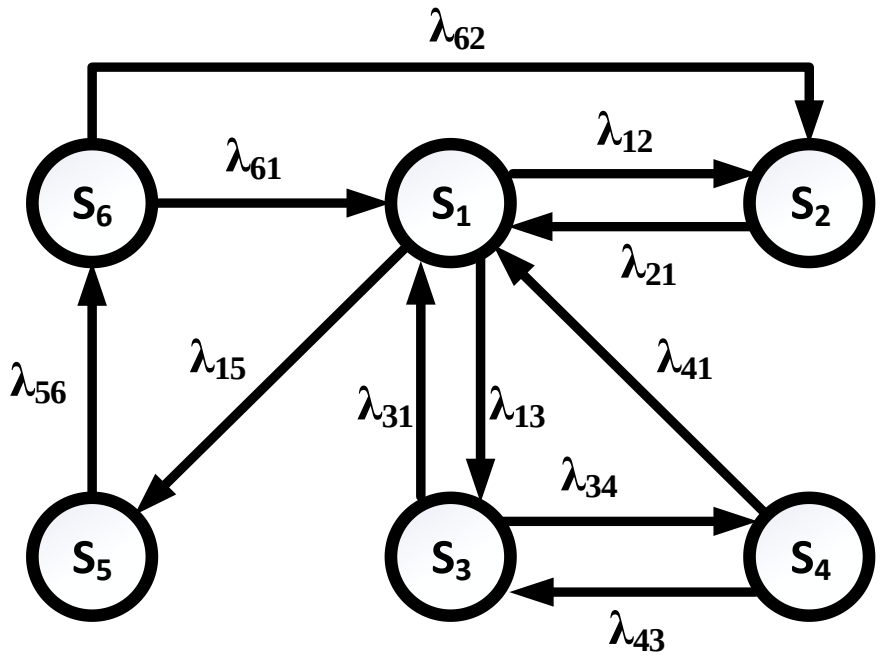
$$\mu:<S, C, Z, I>\rightarrow P_i,\quad Q|\ C\subseteq(A,B),\quad P_i=\lim_{t\rightarrow\infty} P_i(t)$$

Формализованная постановка задачи на оптимизацию показателей эффективности верификации результативности маскирования логической структуры ИС (для минимизации вероятности вскрытия (от англ. *Detection*) структуры ИС средством ТКР):

$$<S, C, Z, I>\rightarrow \min P_D^C=\lim_{t\rightarrow\infty} P_D^C(t)\ |\ P_D^C(t)\in\{P_i\},\ i=1,2,\ldots,h$$

$$C\subseteq\{A,B\}\qquad Z\subseteq\{S_i,\Lambda_j\}\qquad I\subseteq\{TCP,UDP\}\qquad Q=\lim_{t\rightarrow\infty} P_D^C(t)$$

Граф состояний моделируемой системы



Интенсивности потоков событий в ИС

λ_{12} – Поток событий (штатных, протокольных) на продление времени аренды и назначение сетевых параметров новым абонентам ИС от DHCP-сервера
λ_{21} – Поток событий (штатных, протокольных или внеочередных) на подтверждение сетевых параметров абонентами ИС к DHCP-серверу
λ_{13} – Заявки на идентификацию средствами ТКР структурно-функциональных характеристик ИС в диалоговом режиме
λ_{31} – Поток отказов сетевого сканирования ТКР, вызванный функционированием средства защиты логической структуры ИС, и окончание сканирования
λ_{34} – Поток событий на оценку результативности средств ТКР, связанный с успешным окончанием сетевого сканирования
λ_{43} – Поток отказов оценки результативности ТКР, заявки на продолжение ТКР
λ_{15} – Поток событий обнаружения средств ТКР средствами СОВ
λ_{41} – Поток отказов средств СОВ, ИС вскрыта с требуемой ТКР полнотой
λ_{56} – Заявки на оценку результативности защиты от средств ТКР, опасность ТКР, необходимость принятия мер противодействия ТКР
λ_{61} – Поток отказов необходимости менять логическую структуру ИС из-за наличия активных критических соединений или отсутствия необходимости ПД ТКР
λ_{62} – Поток событий на внеочередное изменение сетевых параметров абонентам ИС от DHCP-сервера в связи с недостаточностью результативности защиты от ТКР

Дискретные состояния ИС

S1 – состояние покоя системы. Сетевые параметры абонентам ИС назначены и статичны. Воздействие средств ТКР отсутствует (или нейтрализованы).

S2 – изменение сетевых параметров абонентов КС ИС DHCP-сервером.

S3 – идентификация логической структуры ИС средствами ТКР в диалоговом режиме, средство ТКР осуществляет последовательное выполнение функций сетевого сканера.

S4 – логическая структура ИС вскрыта с некоторой полнотой, оценка результативности ТКР противником.

S5 – обнаружение средств ТКР средствами СОВ.

S6 – оценка возможности изменить структурно-функциональные характеристики, оценка результативности защиты от средств ТКР.

Система дифференциальных уравнений

$$\begin{cases} \frac{dp_1(t)}{dt} = \lambda_{61}p_6(t)+\lambda_{31}p_3(t)+\lambda_{41}p_4(t)+\lambda_{21}p_2(t)-\lambda_{12}p_1(t)-\lambda_{13}p_1(t)-\lambda_{15}p_1(t) \\ \frac{dp_2(t)}{dt} = \lambda_{12}p_1(t)+\lambda_{62}p_6(t)-\lambda_{21}p_2(t) \\ \frac{dp_3(t)}{dt} = \lambda_{13}p_1(t)+\lambda_{43}p_4(t)-\lambda_{31}p_3(t)-\lambda_{34}p_3(t) \\ \frac{dp_4(t)}{dt} = \lambda_{34}p_3(t)-\lambda_{43}p_4(t)-\lambda_{41}p_4(t) \\ \frac{dp_5(t)}{dt} = \lambda_{15}p_1(t)-\lambda_{56}p_5(t) \\ \frac{dp_6(t)}{dt} = \lambda_{56}p_5(t)-\lambda_{61}p_6(t)-\lambda_{62}p_6(t) \\ \sum_{i=1}^{6} p(t)=1 \end{cases}$$

Вектор начального состояния

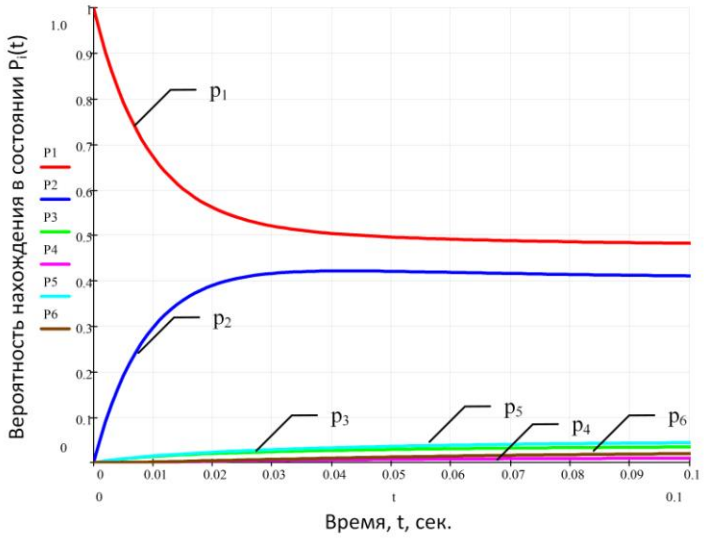
$$p_i(0)=|1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0|$$

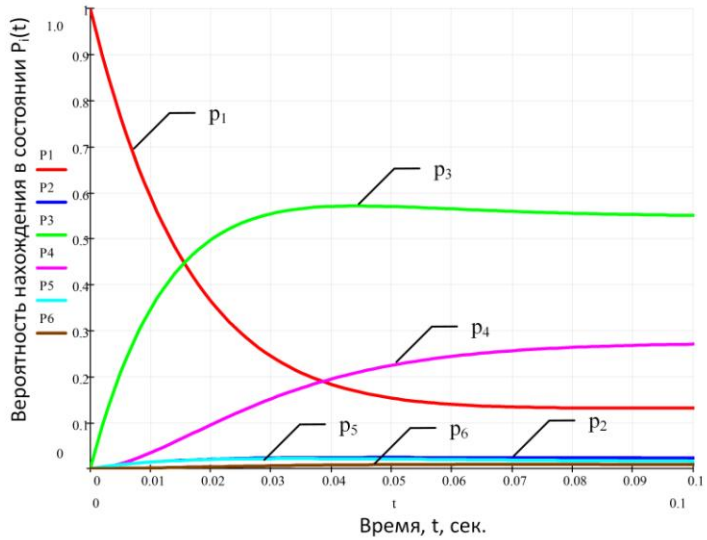
Сумма всех вероятностей состояний

$$\sum_{i=1}^{6} p_i(t)=1$$

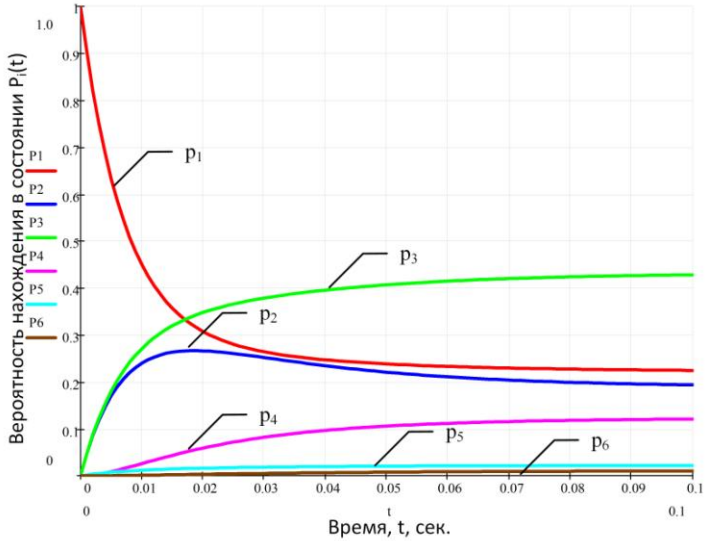
Схема Рунге-Кутты четвертого порядка аппроксимации

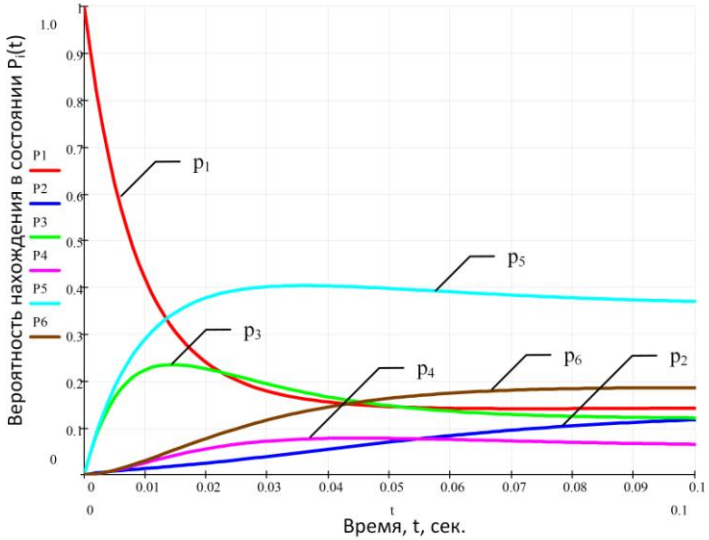
$$\begin{cases} \eta_1^i = S(t_i, p_i) \\ \eta_2^i = S\left(t_i+\frac{h}{2}, p_i+\frac{h}{2}\eta_1^i\right) \\ \eta_3^i = S\left(t_i+\frac{h}{2}, p_i+\frac{h}{2}\eta_2^i\right) \\ \eta_4^i = S(t_i+h, p_i+h\eta_3^i) \\ \Delta p_i = \frac{h}{6}\left(\eta_1^i+2\eta_2^i+2\eta_3^i+\eta_4^i\right) \\ p_{i+1} = p_i+\Delta p_i \end{cases}$$





- Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий, соответствующих стратегиям С1 и С2





- Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий, соответствующих стратегиям С3 и С4

Спасибо за внимание!