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

МОДЕЛЬ И МЕТОДИКА МАСКИРОВАНИЯ АДРЕСАЦИИ КОРРЕСПОНДЕНТОВ В КИБЕРПРОСТРАНСТВЕ

Авторы: Кучуров В.В., Шерстобитов Р.С.

МОДЕЛЬ И МЕТОДИКА МАСКИРОВАНИЯ АДРЕСАЦИИ КОРРЕСПОНДЕНТОВ В КИБЕРПРОСТРАНСТВЕ

- ***Цель*** *исследования – вскрыть и сформулировать основные направления поиска новых технических решений для маскирования структуры распределенных информационных систем в киберпространстве, реализуя маскирующий трафик с учетом требований к своевременности информационного обмена.*
- ***Метод*** *исследования – исследование операций в условиях неопределенности, применение теории марковских случайных процессов и решение уравнений Колмогорова для решения задачи повышения эффективности маскирующего обмена.*
- ***Результат*** *исследования – нахождение вероятностных и временных характеристик процесса функционирования сети передачи данных при применении технических решений по маскированию информационных систем в киберпространстве. Полученные результаты позволяют явно реализовывать меры защиты, направленные на формирование у нарушителей устойчивых ложных стереотипов об информационных системах и процессах управления, реализуемых с их помощью.*

Введение

- **Киберпространство** – это виртуальная сетевая среда, сформированная в результате действий пользователей, программ и сервисов в сети связи общего пользования (ССОП) посредством сетей передачи данных, коммуникационных технологий и информационных систем.
- **Информационные системы (ИС)** – это совокупность территориально распределенных сегментов средств обработки информации, объединенных сетями передачи данных, с использованием коммуникационных технологий через ССОП с целью предоставления пользователям информационных ресурсов (программ и сервисов).

Физическая постановка задачи

- **Наилучшая стратегия защиты** – формировать у нарушителя ложное (неверное) представление о схеме информационных направлений (структуре (топологии) и параметрах (типологии)) ИС и, как неизбежное следствие, структуре системы управления, в интересах которой функционирует распределенная ИС. Это позволяет влиять на качество решений, принимаемых нарушителем по результатам разведки, предотвращать деструктивные воздействия на объекты защиты или снижать их результативность и эффективность.
- **Маскирование адресной информации корреспондентов** – это ее сокрытие путем трансляции (*NAT*, от англ. *Network Address Translation* – «преобразование сетевых адресов») истинных адресов элементов ИС и сети передачи данных (СПД), расширения адресного пространства элементов СПД (увеличение их количества) и введение ложных (маскирующих) элементов в киберпространство.
- **Маскирующий обмен** – это упорядоченная по структуре и интенсивности совокупность ложных (маскирующих) пакетов сообщений, формируемых сетевыми информационными объектами (СИО) с целью управления демаскирующими признаками (ДМП) алгоритмов функционирования ИС и СПД, изменяющих видимую интенсивность информационного обмена между элементами СПД ВН

Физическая постановка задачи

Суть способа	Недостатки	Достоинства
Установка меток в маскирующих пакетах сообщений	Нагрузка на СИО	Реализуется без дополнительных технических решений
Фрагментация маскирующих сообщений перед передачей в СПД и уничтожение одного из фрагментов	Нагрузка на СИО	Реализуется без дополнительных технических решений
Трассировка маршрута IP-пакетов и установление значений TTL (Time To Live) и Hop Limit (для IPv6)	Прямой ДМП в заголовке и косвенный ДМП по протоколу ICMP, низкая результативность	Используют технологии ССОП. Исключают нагрузку на приемник.
Использование Path MTU discovery, установление относительно большого значения MTU и значения флага DF (Do Not Fragment) в «1»	Прямой ДМП в заголовке IPv4, косвенный ДМП по протоколу ICMP, MTU Discovery Black Hole	
Согласование с приемником значения Maximum segment size для маскирующего трафика и управление значением MTU	Косвенный ДМП по протоколу ICMP	

Физическая постановка задачи

Отказ терминации маскирующего трафика может происходить по следующим причинам:

- сбои функционирования СПД вследствие воздействия непреднамеренных помех;
- преднамеренные деструктивные воздействия на СПД (узлы ССОП);
- сбои и ошибки установления значений *MTU* узлом-отправителем;
- маршрутизация пакетов оператором ССОП по альтернативному маршруту;
- изменение параметров и структуры ССОП;
- изменение значений параметров безопасности маршрутов связи;
- изменение ИС (структуры системы управления), которую реализует СПД.

Формализованная постановка задачи на моделирование оценки эффективности маскирующего обмена

- Стратегия защиты при реализации маскирующего обмена должна заключаться в оптимальном распределении ресурса СПД ВН для обеспечения своевременности информационного обмена (доставки сообщений) с учетом приоритетов корреспондентов (видов трафика), предотвращения задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом. При этом производительность СИО и предельная скорость передачи данных в СПД (пропускная способность каналов связи) выступают в качестве очевидных ограничений.

Формализованная постановка задачи на моделирование оценки эффективности маскирующего обмена

- Своевременность информационного обмена (от англ. (*information*) *exchange* – обмен) определяют [8] через показатели своевременности обработки (от англ. *processing* – обработка) и своевременности доставки (от англ. *delivery* – доставка) следующими соотношениями:

$$K_{Proc} = P\ T_{Proc} \le T_{Proc}^{Req}$$

$$K_{Del} = P\ T_{Del} \le T_{Del}^{Req}$$

$$K_{IE} = K_{Del} \cdot K_{Proc}$$

Формализованная постановка задачи на моделирование оценки эффективности маскирующего обмена

S – сеть передачи данных военного назначения (СДП ВН)

CP – множество входных параметров модели, параметры контроля насыщения соединения $CP \subseteq N_T, I^{AT}, I^{CT}, I^{MT}$

где N_T – узел-терминатор МПС (от англ. *Node* – узел, *Terminator* – оконечное устройство); I^{AT}, I^{CT}, I^{NT} – расчетная интенсивность общего трафика, конструктивного трафика, маскирующего трафика (от англ. *Intensity* – интенсивность);

P_i – множество выходных параметров модели, значения финальных вероятностей состояний системы *S*, $P_i = \lim_{t \to \infty} P_i \ t$

где $i = 1, 2, \ldots, h$, причем число состояний конечно и из каждого из них можно за конечное число шагов перейти в любое другое;

Z – множество внутренних параметров модели $Z \subseteq S_i, \Lambda_j$

где $S_i = \{S_1, \ldots, S_h\}$, $\Lambda_j = \{\lambda_1, \lambda_2, \ldots, \lambda_J\}$, перечень моделируемых состояний системы и интенсивностей потоков событий

SIT – множество параметров условий функционирования (ситуаций), поддерживаемые моделируемой системой

$SIT \subseteq I^{OT}, I^{FT}$

где $\boldsymbol{I^{OT}}$ – моделируемая интенсивность трафика КПС других источников (от англ. *Other* – другой, дополнительный);
$\boldsymbol{I^{FT}}$ – моделируемая интенсивность отказов узла-терминатора (от англ. *Failure* – отказ), выражаемая, например, через коэффициент $I^{FT} = \lambda_{57} / \lambda_{45}$

Q – показатель эффективности функционирования СПД ВН,

$Q = \lim_{t \to \infty} P^{K_{IE}} \ t \qquad P^{K_{IE}} \ t \ \to \max$

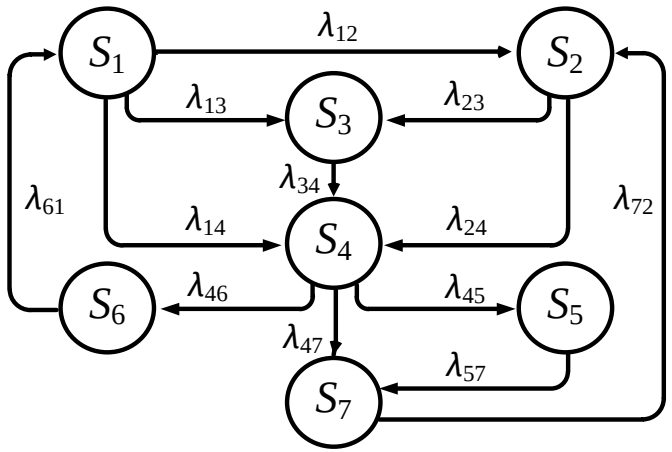
определяемый своевременностью информационного обмена.

$$\mu : < S, CP, \ Z, SIT > \to P_{i,} Q \,|\, CP \subseteq N_T, I^{AT}, I^{CT}, I^{MT} \ , \ P_i = \lim_{t \to \infty} P_i \ t \ , \ SIT \subseteq I^{OT}, I^{FT}$$

$$< S, CP, \ Z, SIT > \to \max P^{K_{IE}} \ t \ | \ P^{K_{IE}} \in P_i \ , i = 1, 2, \ldots, h$$

Модель оценки эффективности маскирующего обмена в киберпространстве

Граф состояний процесса функционирования СПД ВН при реализации маскирующего обмена



$$\frac{dp_1(t)}{dt} = \lambda_{61} p_6(t) - \lambda_{12} p_1(t) - \lambda_{13} p_1(t) - \lambda_{14} p_1(t),$$

$$\frac{dp_2(t)}{dt} = \lambda_{12} p_1(t) + \lambda_{72} p_7(t) - \lambda_{23} p_2(t) - \lambda_{24} p_2(t),$$

$$\frac{dp_3(t)}{dt} = \lambda_{13} p_1(t) + \lambda_{23} p_2(t) - \lambda_{34} p_3(t),$$

$$\frac{dp_4(t)}{dt} = \lambda_{14} p_1(t) + \lambda_{24} p_2(t) + \lambda_{34} p_3(t) - (\lambda_{45} + \lambda_{46} + \lambda_{47}) p_4(t),$$

$$\frac{dp_5(t)}{dt} = \lambda_{45} p_4(t) - \lambda_{57} p_5(t),$$

$$\frac{dp_6(t)}{dt} = \lambda_{46} p_4(t) - \lambda_{61} p_6(t),$$

$$\frac{dp_7(t)}{dt} = \lambda_{47} p_4(t) + \lambda_{57} p_5(t) - \lambda_{72} p_7(t),$$

$$\sum_{i=1}^{7} p_i(t) = 1.$$

Дискретные состояния процесса маскирования СПД ВН

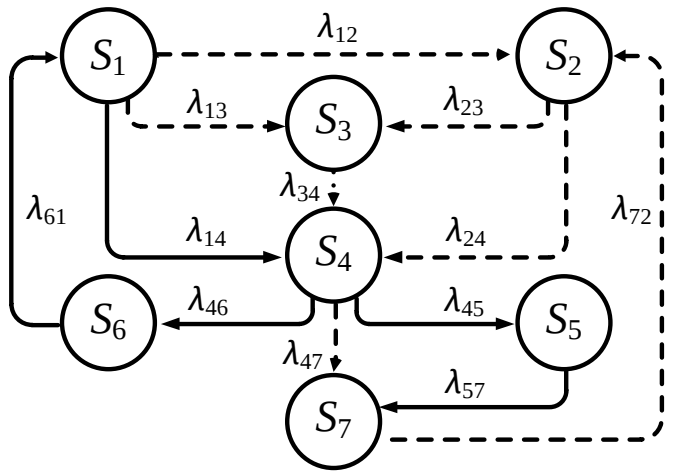
S_1 - Формирование конструктивных пакетов сообщений (КПС)
S_2 - Формирование маскирующих пакетов сообщений (МПС)
S_3 - Изменение текущих *IP*-адресов (расширение адресного пространства) элемента СПД ВН
S_4 - Передача КПС и МПС от отправителя к получателю
S_5 - Терминация МПС на транзитном УС СПД ССОП
S_6 - Своевременный прием КПС
S_7 - Несвоевременный прием КПС

Интенсивности потоков событий

λ_{12} - Заявки на прерывание формирования МПС в связи с формированием КПС
λ_{13} - Заявки на изменение текущих *IP*-адресов (расширение адресного пространства) КПС
λ_{23} - Заявки на изменение текущих *IP*-адресов (расширение адресного пространства) МПС
λ_{14} - Заявки на передачу КПС получателю без расширения адресного пространства (КПС и МПС используют один адрес отправителя)
λ_{24} - Заявки на передачу МПС получателю без расширения адресного пространства (МПС и КПС используют один адрес отправителя)
λ_{34} - Заявки на передачу КПС и МПС получателю с расширением адресного пространства (КПС и МПС используют множество адресов отправителя)
λ_{45} - Заявки на терминацию МПС на узле-терминаторе
λ_{46} - Заявки на приоритетное обслуживание КПС у получателя
λ_{47} - Заявки на совместное с МПС обслуживание КПС у получателя
λ_{57} - Заявки на совместное с КПС обслуживание МПС у получателя, вызванные отказом терминации (узла-терминатора)
λ_{61} - Квитирование, заявки на увеличение скорости ПД КПС вследствие своевременного приема КПС
λ_{72} - Заявки на уменьшение скорости ПД МПС вследствие отказа терминации, возникновения очередей из КПС и МПС у получателя

Модель оценки эффективности маскирующего обмена в киберпространстве

Граф состояний процесса функционирования СПД ВН при реализации маскирующего обмена для λ ситуации C_1



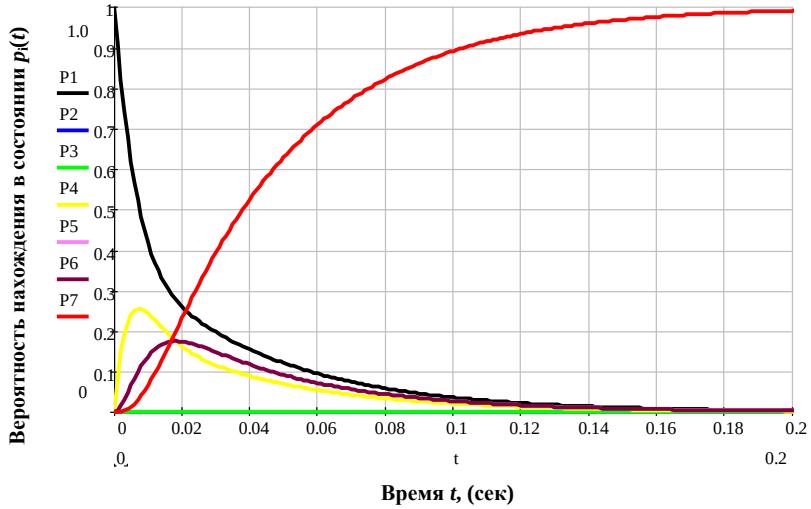
Ситуация C_1

Формирование, передача и прием только КПС, МПС не формируется. Тогда поток КПС к приемнику интерпретируется как КПС других источников.

Ситуация позволяет исследовать СПД ВН без нагрузки источника МПС и найти максимальную интенсивность (скорость ПД) КПС. При вариации λ_{45} (λ_{57}) исследуется обеспечение своевременности при росте трафика (КПС) от других источников.

Числовая таблица приближенных значений $p_i(t)$ для λ ситуации C_1

Этапы интегрирования, n	Точка интервала интегрирования, $[t_0, t_1]$	$p(t)$						
		$p_1(t)$	$p_2(t)$	$p_3(t)$	$p_4(t)$	$p_5(t)$	$p_6(t)$	$p_7(t)$
1	0	1	0	0	0	0	0	0
2	$1\cdot10^{-3}$	0,905	0	0	0,086	$4{,}379\cdot10^{-3}$	$4{,}379\cdot10^{-3}$	$1{,}5\cdot10^{-4}$
3	$2\cdot10^{-3}$	0,82	0	0	0,148	0,015	0,015	$1{,}092\cdot10^{-3}$
…	…	…	…	…	…	…	…	…
10^3	10	$1{,}654\cdot10^{-4}$	0	0	$9{,}423\cdot10^{-5}$	$1{,}248\cdot10^{-4}$	$1{,}248\cdot10^{-4}$	0,999

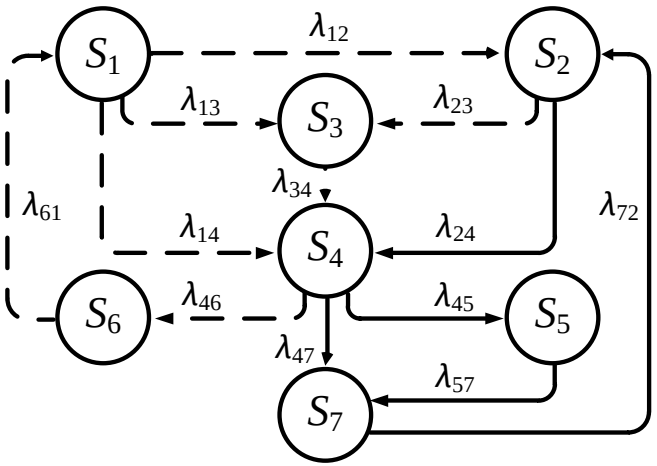


Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий соответствующие ситуации C_1

$$\sum_{i=1}^{7} p_i(10) = 1{,}654\cdot10^{-4} + 9{,}423\cdot10^{-5} + 1{,}248\cdot10^{-4} + 1{,}248\cdot10^{-4} + 0{,}999 = 1$$

Модель оценки эффективности маскирующего обмена в киберпространстве

Граф состояний процесса функционирования СПД ВН при реализации маскирующего обмена для λ ситуации C_2



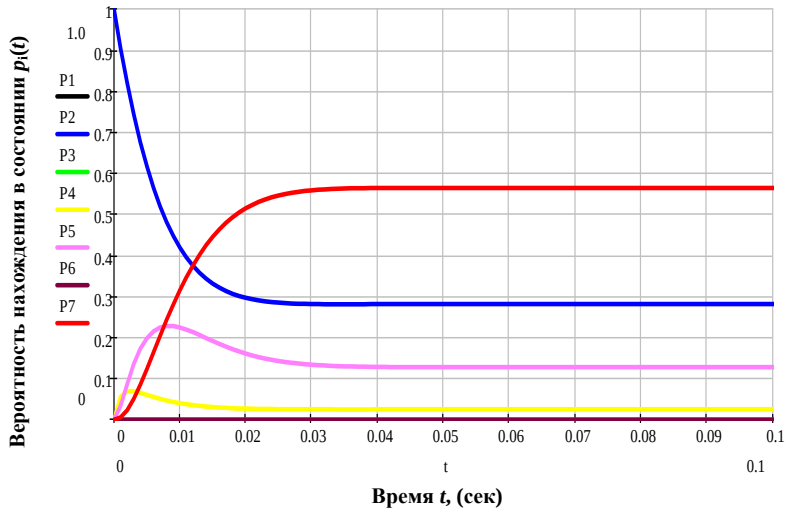
Ситуация C_2

Формирование, передача и прием только МПС (без терминации МПС), получателю КПС не передаются. КПС заданной (плановой) интенсивности от других источников. λ_{45}=max (искомое).

Ситуация позволяет исследовать СПД ВН без нагрузки источника КПС и найти максимальную интенсивность λ_{45} (скорость ПД) МПС при наличии заданного трафика от других источников. При увеличении λ_{45} находим предел обеспечения своевременности при увеличении МПС.

Числовая таблица приближенных значений $p_i(t)$ для λ ситуации C_2

Этапы интегрирования, n	Точка интервала интегрирования, $[t_0, t_1]$	$p(t)$						
		$p_1(t)$	$p_2(t)$	$p_3(t)$	$p_4(t)$	$p_5(t)$	$p_6(t)$	$p_7(t)$
1	0	0	1	0	0	0	0	0
2	$1\cdot10^{-3}$	0	0,905	0	0,056	0,033	0	$5{,}622\cdot10^{-3}$
3	$2\cdot10^{-3}$	0	0,819	0	0,07	0,087	0	0,023
…	…	…	…	…	…	…	…	…
10^3	10	0	0,282	0	0,026	0,128	0	0,564

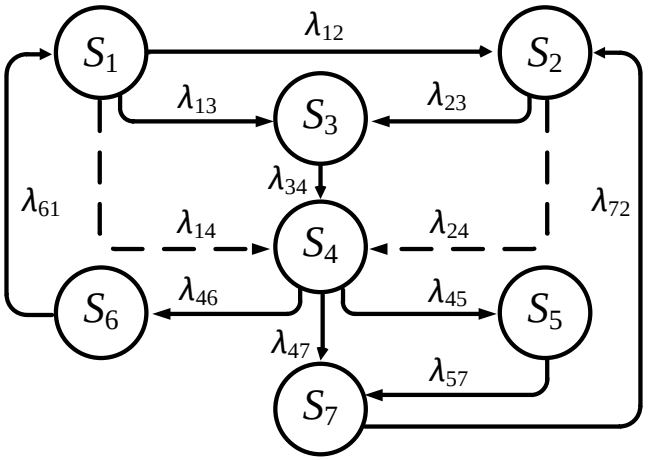


Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий соответствующие ситуации C_2

$$\sum_{i=1}^{7} p_i(10) = 0,282 + 0,026 + 0,128 + 0,564 = 1$$

Модель оценки эффективности маскирующего обмена в киберпространстве

Граф состояний процесса функционирования СПД ВН при реализации маскирующего обмена для λ ситуации C_3



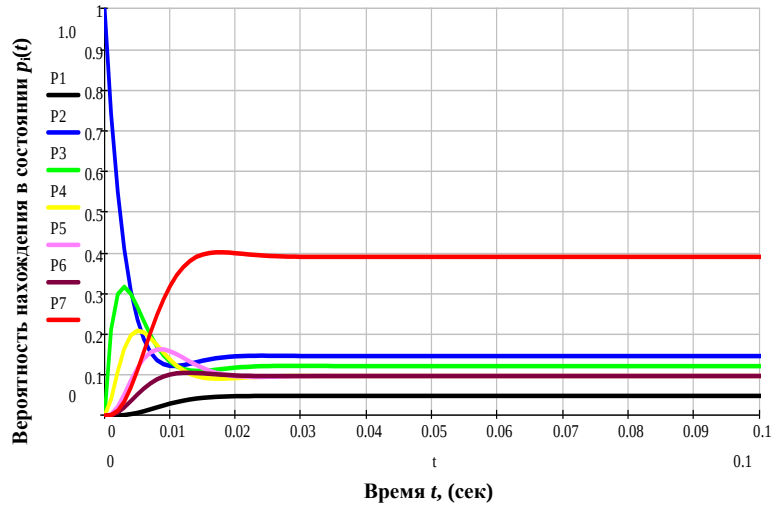
Ситуация C_3

Формирование, передача и прием МПС и КПС заданной (плановой) интенсивности.

Ситуация позволяет исследовать предел обеспечения своевременности при увеличении МПС (без терминации МПС).

Числовая таблица приближенных значений $p_i(t)$ для λ ситуации C_3

Этапы интегрирования, n	Точка интервала интегрирования, $[t_0, t_1]$	$p(t)$						
		$p_1(t)$	$p_2(t)$	$p_3(t)$	$p_4(t)$	$p_5(t)$	$p_6(t)$	$p_7(t)$
1	0	0	1	0	0	0	0	0
2	$1\cdot10^{-3}$	$5\cdot10^{-5}$	0,741	0,211	0,041	$3{,}75\cdot10^{-3}$	$1{,}35\cdot10^{-3}$	$1{,}8\cdot10^{-3}$
3	$2\cdot10^{-3}$	$4{,}5\cdot10^{-4}$	0,549	0,298	0,109	0,022	$8{,}333\cdot10^{-3}$	0.012
…	…	…	…	…	…	…	…	…
10^3	10	0,049	0,146	0,122	0,098	0,098	0,098	0,39

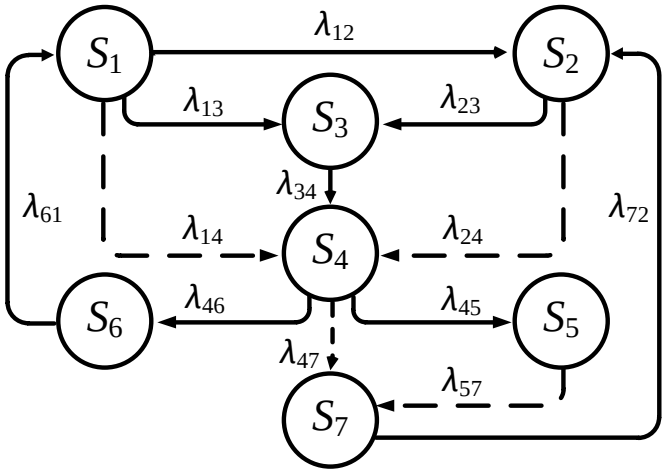


Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий соответствующие ситуации C_3

$$\sum_{i=1}^{7} p_i(10) = 0{,}049 + 0{,}146 + 0{,}122 + 0{,}098 + 0{,}098 + 0{,}098 + 0{,}39 = 1$$

Модель оценки эффективности маскирующего обмена в киберпространстве

Граф состояний процесса функционирования СПД ВН при реализации маскирующего обмена для λ ситуации C_4



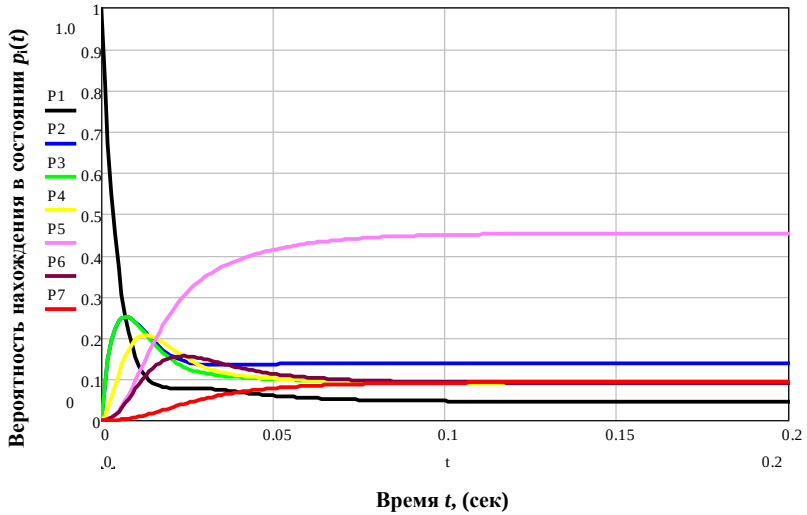
Ситуация C_4

Формирование, передача и прием МПС и КПС заданной (плановой) интенсивности.

Ситуация позволяет исследовать предел обеспечения своевременности при увеличении МПС с терминацией, предел сбоев терминации МПС для обеспечения своевременности.

Числовая таблица приближенных значений $p_i(t)$ для λ ситуации C_4

Этапы интегрирования, n	Точка интервала интегрирования, $[t_0, t_1]$	$p(t)$						
		$p_1(t)$	$p_2(t)$	$p_3(t)$	$p_4(t)$	$p_5(t)$	$p_6(t)$	$p_7(t)$
1	0	1	0	0	0	0	0	0
2	$1\cdot10^{-3}$	0,819	0,086	0,086	$8,47\cdot10^{-3}$	$2,898\cdot10^{-4}$	$2,832\cdot10^{-4}$	$7,33\cdot10^{-6}$
3	$2\cdot10^{-3}$	0,67	0,148	0,148	0,029	$2,055\cdot10^{-3}$	$1,97\cdot10^{-3}$	$6,049\cdot10^{-5}$
…	…	…	…	…	…	…	…	…
10^{3}	10	0,045	0,138	0,091	0,09	0,452	0,09	0,092



Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий соответствующие ситуации C_4

$$\sum_{i=1}^{7} p_i(10) = 0,045 + 0,138 + 0,091 + 0,09 + 0,452 + 0,09 + 0,092 = 1$$

Выводы

- Представленная математическая модель оценки эффективности маскирующего обмена в киберпространстве учитывает влияние и характер воздействия на СПД информационных потоков от передающего к принимающему абоненту, фоновую нагрузку ИС, отказы системы маскирования, которые способны снизить доступность принимающего абонента и ухудшить значение показателя своевременности информационного обмена в ИС.
- **Научная новизна** модели заключается в применении математического аппарата теории марковских случайных процессов и решении уравнений Колмогорова для исследования и решения задачи повышения эффективности маскирующего обмена при маскировании адресации корреспондентов в киберпространстве за счет обеспечения своевременности информационного обмена конструктивными сообщениями.
- **Практическая значимость** заключается в нахождении вероятностных и временных характеристик, описывающих состояния процесса функционирования сети передачи данных в различных условиях, которые необходимо использовать при синтезе ложных информационных систем для решения задач дезинформации нарушителя относительно архитектуры и конфигурации объектов защиты.