Модель и методика маскирования адресации корреспондентов в сети передачи данных ведомственного назначения

В. В. Кучуров, email: kuchurovv@yandex.ru
Р. С. Шерстобитов, email: scherstobitov.rs@yandex.ru

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

Аннотация. *Для выполнения требований по защите информации предписанных регуляторами, возникает необходимость по противодействию угрозам безопасности информации, нацеленным на вскрытие структурно-функциональных характеристик информационной системы (ИС). Такая стратегия защиты может быть реализована посредством маскирования адресации корреспондентов и осуществления маскирующего обмена между топологически локализованными элементами (сегментами) СПД ВН.*

Ключевые слова: *moving target defense, компьютерная разведка, информационные направления, маскирование сетевых адресов, марковские процессы, маскирующий обмен*.

Введение

Как правило, каждая локализованная (топологически) ИС функционирует в интересах конкретного органа управления, являющегося элементом иерархичной системы управления [1].

В ведомственных ИС кибербезопасность и защита киберпространства реализуется как набор мер и рекомендаций ФСТЭК. В значимых ИС объектами, подлежащими защите от угроз безопасности информации, являются архитектура и конфигурация ИС (равно как и архитектура и конфигурация информационно-телекоммуникационной сети, АСУ).

По результатам анализа защищенности должно быть подтверждено, что в ИС отсутствуют уязвимости, способствующие возможности реконструкции (вскрытия) нарушителем архитектура и конфигурация ИС. [3].

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). При этом производительность СИО и предельная скорость передачи данных в СПД (пропускная способность каналов связи) выступают в качестве очевидных ограничений [4].

Своевременность информационного обмена K_{IE} (от англ. (information) exchange – обмен) определяют [8] через показатели своевременности обработки K_{Proc} (от англ. processing – обработка) и своевременности доставки K_{Del} (от англ. delivery – доставка) следующими соотношениями:

$$K_{Proc} = P\left(T_{Proc} \le T_{Proc}^{Req}\right) \quad (1)$$

$$K_{Del} = P\left(T_{Del} \le T_{Del}^{Req}\right) \quad (2)$$

$$K_{IE} = K_{Del} \cdot K_{Proc} \quad (3)$$

Время обработки T_{Proc} и время доставки T_{Del} являются контекстно-зависимыми величинами, то есть требуют достаточно точно определять состав канала (каналов) связи СПД ВН, конкретизировать функции СИО и процессов обработки (доставки) относительно уровней ЭМВОС.

Тогда коэффициент эффективности маскирующего обмена в i-ом информационном направлении:

$$K_i^{Ef} = \frac{\overline{T}_{IE}^{AT} - \overline{T}_{IE}^{CT}}{\overline{T}_{IE}^{AT}} \quad (4)$$

где $\overline{T}_{IE}^{AT}$ – среднее время информационного обмена общим трафиком (КПС и МПС); $\overline{T}_{IE}^{CT}$ – среднее время информационного обмена конструктивным трафиком при ограничении МПС узлами-терминаторами.

Моменты возможных переходов СПД из состояния в состояние неопределенны и случайны. Рассмотрим переход от детерминированной постановки задачи к постановке задачи в условиях неопределенности. Тогда финальную вероятность того или иного состояния S_i СПД ВН

можно будет интерпретировать как среднее относительное время пребывания системы в этом состоянии.

Тогда содержательная постановка задачи на моделирование оценки эффективности маскирующего обмена в СПД при маскировании адресации корреспондентов в киберпространстве: разработать модель μ СПД S, устанавливающую закономерность изменения множества P_i выходных параметров модели функционирования СПД и множества Q показателей эффективности функционирования СПД от множества CP значений входных параметров, множества Z значений внутренних параметров, множества SIT значений параметров условий функционирования. На значения параметров множеств CP, P_i, Z, SIT наложены условия их допустимости.

Тогда формальная постановка задачи на моделирование оценки эффективности маскирующего обмена в СПД при маскировании адресации корреспондентов в киберпространстве:

$$\begin{gathered} \mu : \left\langle S, CP, Z, SIT \right\rangle \to P_i, \\ Q \left| CP \subseteq \left\{ N_T, I^{AT}, I^{CT}, I^{MT} \right\}, \right. \\ P_i = \lim_{t \to \infty} P_i(t), SIT \subseteq \left\{ I^{OT}, I^{FT} \right\} \end{gathered} \tag{5}$$

а формальная постановка задачи на оптимизацию показателей эффективности маскируемой СПД (по критерию максимизации своевременности информационного обмена):

$$< S,\ CP, Z,\ SIT\ > \to \max P^{K_{ИС}}(t) \mid P^{K_{ИС}} \in \{P_i\},\ i = 1,\ 2, \ldots,\ h \tag{6}$$

Модель оценки эффективности маскирующего обмена в сети передачи данных ведомственного назначения

Пусть имеется СПД ВН S, в которой реализуют маскирование адресации корреспондентов и осуществление маскирующего обмена между топологически локализованными элементами (сегментами) распределенной ИС. [5]

От передающих абонентов в СПД ВН и далее в ССОП поступает поток событий (заявок, требований) с интенсивностью λ, потенциально переводящих модель μ СПД S в состояния, когда обеспечивается или не обеспечивается своевременность информационного обмена.

Примем следующие необходимые для исследования дискретные состояния $S_1, S_2, \cdots$ моделируемого процесса, где: S_1 – формирование КПС, S_2 – формирование МПС, S_3 – изменение текущих IP-адресов элемента СПД (расширение его адресного пространства), S_4 – передача

КПС и МПС от отправителя к получателю, s_5 – терминация МПС на транзитном СИО СПД в ССОП, s_6 – своевременный прием КПС, s_7 – несвоевременный прием КПС.

Моменты возможных переходов моделируемой СПД при реализации маскирующего обмена из состояния в состояние неопределенны, случайны и происходят под действием событий, характеризующиеся их интенсивностями λ (см. табл. 2).

Таблица 1

Интенсивности потоков событий

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

Оценка эффективности процессов функционирования СПД ВН и маскирования адресации корреспондентов связана с необходимостью моделирования процесса в реальном времени, что обусловливает целесообразность использования математического аппарата марковских процессов. Таким образом, процессы маскирования адресации корреспондентов при реализации маскирующего обмена можно представить, как марковский случайный процесс с дискретными состояниями и непрерывным временем.

На рис. 1 представлен граф состояний моделируемой системы. Рассмотрим сценарий перехода моделируемой системы из состояния s_i в состояние s_j под воздействием потоков событий с интенсивностями λ_{ij}.

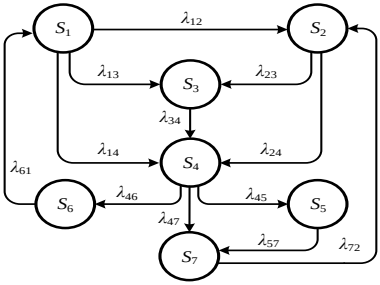

Рис. 1. Граф состояний процесса функционирования моделируемой системы

Пусть формирование МПС происходит постоянно, чтобы скрывать факт передачи КПС, тогда s_2 – начальное состояние моделируемой системы. Это состояние обеспечивает результативность маскирования, интенсивность которого определяется для каждого информационного направления по модели, изложенной в [2], и является искомым с позиций обеспечения результативности [7] маскирования (то есть интенсивность λ_{23} (λ_{24}) такова, что требования по интенсивности маскирующего обмена выполняются).

Моделируемая СПД может находиться в состояниях s_i с разной вероятностью $p_i(t)$. По размеченному графу состояний рис.1 составлены уравнения Колмогорова – дифференциальные уравнения с неизвестными функциями $p_i(t)$:

$$
\left.
\begin{aligned}
&\frac{dp_1(t)}{dt} = \lambda_{61} p_6(t) - \lambda_{12} p_1(t) - \lambda_{13} p_1(t) - \lambda_{14} p_1(t),\\
&\frac{dp_2(t)}{dt} = \lambda_{12} p_1(t) + \lambda_{72} p_7(t) - \lambda_{23} p_2(t) - \lambda_{24} p_2(t),\\
&\frac{dp_3(t)}{dt} = \lambda_{13} p_1(t) + \lambda_{23} p_2(t) - \lambda_{34} p_3(t),\\
&\frac{dp_4(t)}{dt} = \lambda_{14} p_1(t) + \lambda_{24} p_2(t) + \lambda_{34} p_3(t) - (\lambda_{45} + \lambda_{46} + \lambda_{47}) p_4(t),\\
&\frac{dp_5(t)}{dt} = \lambda_{45} p_4(t) - \lambda_{57} p_5(t),\\
&\frac{dp_6(t)}{dt} = \lambda_{46} p_4(t) - \lambda_{61} p_6(t),\\
&\frac{dp_7(t)}{dt} = \lambda_{47} p_4(t) + \lambda_{57} p_5(t) - \lambda_{72} p_7(t),\\
&\sum_{i=1}^{7} p_i(t) = 1.
\end{aligned}
\right\} \qquad (7)
$$

Вектор вероятностей начальных состояний марковской цепи с учетом отсутствия воздействий на СПД в начальный момент времени имеет вид:

$$p(0) = \left| 0 \;\; 1 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \right| \qquad (8)$$

что соответствует формированию МПС.

Задавая численные значения интенсивностей λ в соответствии с условиями функционирования ИС и СПД ВН в ССОП (ситуациями SIT) и переходя к непрерывному времени, решается система линейных дифференциальных уравнений (7) с постоянными коэффициентами. [6] Для решения уравнений численным методом очевидным является классический метод четвертого порядка – метод Рунге-Кутты с фиксированным шагом интегрирования. Применение модели заключается в вариации интенсивностей в пределах устойчивости уравнений, при этом контрастны следующие четыре ситуации λ_{47} (см. таблицу 3).

Таблица 2

Вариация параметров модели в зависимости от условий функционирования СПД

Признаки	**Ситуации**			
	SIT_1	SIT_2	SIT_3	SIT_4
Наличие КПС	const	–	const	const
Наличие МПС	–	max	max	max
Наличие КПС от других источников	max	const	const	const
Терминация МПС	–	min	min	max

Ситуация SIT_1 . Формирование, передача и прием только КПС. Если МПС не формируются. Тогда поток КПС к приемнику постоянный. $\lambda_{45} = \lambda_{57}$ интерпретируется как КПС других источников. Ситуация позволяет исследовать СПД без нагрузки источника МПС и найти максимальную скорость передачи. При вариации λ_{45} (λ_{57}) исследуют обеспечение своевременности при росте трафика от других источников.

Графики зависимостей вероятностей состояний исследуемого процесса для ситуации SIT_1 представлены на рис. 2.

На интервале времени [0; 0,09] СПД находится в переходном режиме функционирования, где наблюдается всплеск значений вероятности состояний $p_4(t)$ и $p_6(t)$ что соответствует нахождению СПД в состоянии передачи, приема КПС и квитирования. При $t \to \infty$ в СПД устанавливается стационарный режим, когда СПД случайным образом меняет свои состояния и ее вероятности $p_1(t), p_2(t), \ldots, p_7(t)$, уже не зависят от времени и равны финальным (предельным) вероятностям.

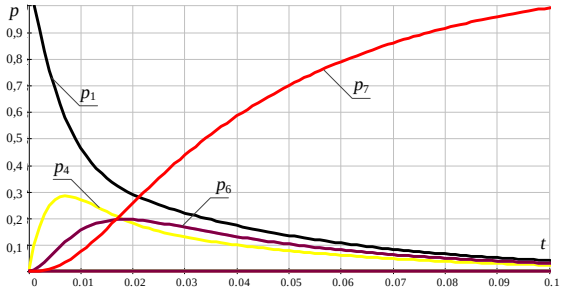

Рис. 2. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий, соответствующие ситуации SIT_1

Аналогично производят расчеты и для остальных ситуаций. Графики зависимостей вероятностей состояний исследуемого процесса для ситуаций SIT_2 – SIT_4 представлены на рисунках 3 – 5.

Ситуация SIT_2 . Формирование, передача и прием только МПС (без их терминации), конструктивные не передаются. $\lambda_{23} = \min$ (λ_{23} и λ_{24} – антагонисты, т.к. или варьируем текущие адреса элемента СПД, или

нет). λ_{57} и λ_{47} интерпретируется как КПС заданной (плановой) интенсивности от других источников. $\lambda_{45} = max$ (искомое). Ситуация позволяет исследовать СПД без нагрузки источника КПС и найти максимальную скорость передачи (см. интенсивность λ_{45}) МПС при наличии заданного трафика от других источников. При увеличении λ_{45} находим предел обеспечения своевременности при увеличении скорости передачи МПС.

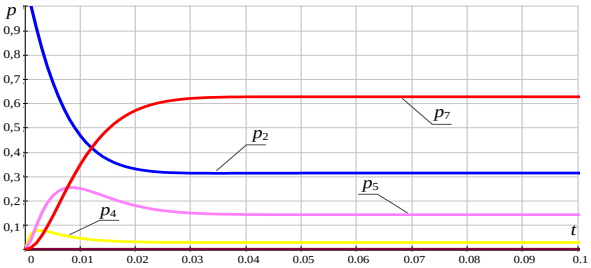

Рис. 3. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий, соответствующие ситуации SIT_2

Ситуация SIT_3. Формирование, передача и прием маскирующих и КПС заданной (плановой) интенсивности. Ситуация позволяет исследовать предел обеспечения своевременности при увеличении скорости передачи МПС.

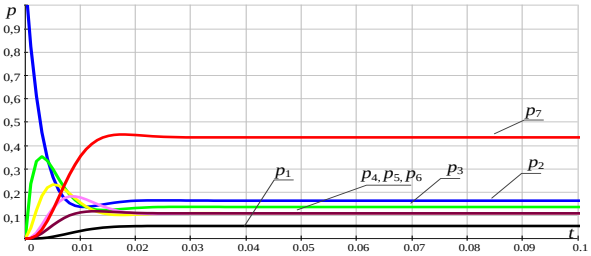

Рис. 4. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий, соответствующие ситуации SIT_3

Ситуация SIT_4. Формирование, передача и прием МПС и КПС заданной (плановой) интенсивности. Ситуация позволяет исследовать предел обеспечения своевременности при увеличении скорости передачи МПС с их терминацией, предел сбоев терминации для обеспечения своевременности.

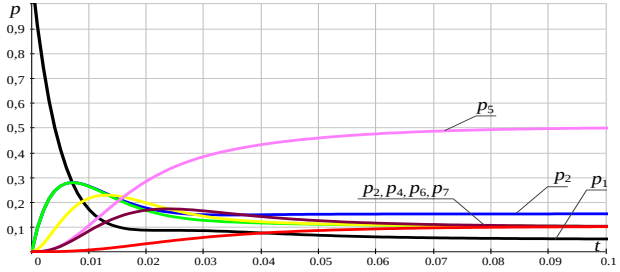

Рис. 5. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий, соответствующие ситуации SIT_4

Конструктивное использование модели очевидным образом приводит к методике маскирования адресации корреспондентов в СПД ВН, в частности, при реализации ложных информационных систем [8]. Процесс защиты принимающего абонента (СИО) от перегрузки в соответствии с методикой сводится к максимизации $p_6(t)$ вероятности (и среднего времени) значения показателя своевременности информационного обмена $P^{K_{ИС}}(t) \to \max$, что предполагает адаптивное управление ложным трафиком при условии выполнения требований к результативности маскирующего обмена [9].

Заключение

Представленная математическая модель оценки эффективности маскирующего обмена в СПД ВН 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.

Список литературы

1. Давыдов, А.Е. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем / А. Е. Давыдов, Р. В. Максимов, О. К. Савицкий – Москва: ОАО «Воентелеком», 2015. – 520 с.
2. Соколовский, С.П. Модель защиты информационной системы от сетевой разведки динамическим управлением ее структурно-функциональными характеристиками // Вопросы оборонной техники. Серия 16 противодействие терроризму. – Москва: 2020. № 7-8. – С. 62-73.
3. Максимов, Р. В. Алгоритм и технические решения динамического конфигурирования клиент-серверных вычислительных сетей / Р. В. Максимов, С. П. Соколовский, И. С. Ворончихин // Труды СПИИРАН. – 2020. – Т. 19. – № 5. – С. 1018-1049.
4. Максимов, Р. В. Модель и алгоритм функционирования клиент-серверной информационной системы в условиях сетевой разведки / Р. В. Максимов, Д.Н. Орехов, С.П. Соколовский // Системы управления, связи и безопасности. – СПб.: 2019. – № 4. – С. 50–99.
5. Ворончихин, И. С. Маскирование структуры распределенных информационных систем в киберпространстве / И. С. Ворончихин [и др.] // Вопросы кибербезопасности. – 2019. – № 6 (34). – С. 92–101.
6. Искольный, Б. Б. Оценка живучести распределенных информационно-телекоммуникационных сетей / Б. Б. Искольный, Р. В. Максимов, С. Р. Шарифуллин // Вопросы кибербезопасности. – 2017. – № 5 (24). – С. 72-82.
7. Максимов, Р. В. Особенности детектирования и способы маскирования демаскирующих признаков средств проактивной защиты вычислительных сетей / Р. В. Максимов, С. П. Соколовский, Д. Н. Орехов // Радиолокация, навигация, связь : сб. тр. XXIV Международной научно-технической конференции. (Воронеж, 17-19 апреля 2018 г.). – Воронеж, 2018. – С. 169-179.
8. Способ маскирования структуры сети связи. Пат. 26822105 Рос. Федерация, МПК G06F / Зайцев Д.В., Зуев О.Е., Крупенин А.В., Максимов Р.В., Починок В.В., Шарифуллин С.Р., Шерстобитов Р.С.; заявитель и патентообладатель Краснодарское высшее военное училище (RU). – № 2018112925; заявл. 09.04.2018; опубл. 14.03.2019, Бюл. № 8.
9. Шерстобитов, Р. С. Маскирование интегрированных сетей связи ведомственного назначения / Р.С. Шерстобитов, С.Р. Шарифуллин, Р.В. Максимов // Системы управления, связи и безопасности. – 2018. – № 4. – С. 136–175.