Модель верификации результативности маскирования структуры информационных систем

М. А. Каплин, email: popi901@yandex.ru [1]

[1] Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М.Штеменко

Аннотация. *В данной статье рассматривается актуальность защиты информационных систем от компьютерных атак, носящих разведывательный характер, представлена постановка задачи на моделирование процесса верификации результативности маскирования структуры информационной системы и ее математическая модель.*

Ключевые слова: *Информационная система, техническая компьютерная разведка, маскирование.*

Введение

В настоящий момент большая доля потребностей в передаче информации в распределенных информационных системах удовлетворяется путем использования универсальной транспортной сети – сети связи общего пользования (ССОП).

Упрощенная архитектура информационной системы (ИС) представляет собой совокупность территориально распределенных локальных сетей (сегментов), объединенных каналами связи через ССОП с использованием коммуникационного оборудования. Основным решением, применяемым в ИС на сетевом и межсетевом уровнях, является использование единого межсетевого протокола IP, обеспечивающего интеграцию услуг во всех составляющих цифровой системы связи.

Передача данных между сегментами ИС осуществляется посредством создания так называемых «криптотуннелей» с использованием технологии «виртуальных частных сетей» (VPN). Причем информация о применяемых транспортных протоколах передается в незашифрованном виде.

Данный факт предоставляет целый спектр демаскирующих признаков ИС, необходимых технической компьютерной разведке (ТКР) для построения модели объекта защиты [1].

Обобщенная модель утечки информации представляется как объединение локальных вычислительных сетей посредством ССОП, находящейся под контролем технических средств ТКР.

Расположение технических средств ТКР противника между защищаемыми сегментами ИС формирует так называемые виртуальные точки присутствия.

Довольно часто компьютерные атаки проводятся с целью получения злоумышленником сведений о применяемом оборудовании, применяемых средствах защиты и средствах обнаружения вторжений, структуре и топологии ИС, а также интенсивностях информационного обмена. Такие атаки носят, прежде всего, разведывательный характер, и предшествуют атакам типа программного подавления, контроля событий и перехвата управления.

В общем случае ИС представляет собой совокупность ЭВМ, периферийного и коммуникационного оборудования, объединенного физическими линиями связи. Все эти элементы определяются идентификаторами, в качестве которых в наиболее распространенном семействе протоколов TCP/IP используются сетевые адреса (IP-адреса).

Для передачи информации между клиентами и серверами в ИС с клиент-серверной архитектурой посредством протоколов взаимодействия устанавливают логическое соединение, под которым понимают инициализацию (передача пакета с установленным флагом SYN) запросов на обслуживание (информационных потоков) от клиента к серверу, получение параметров соединения и поддержание соединения между клиентом и сервером до его окончания. Применяя режим автоматического распределения динамических параметров соединения [2], сетевые параметры, полученные от сервера клиентами будут меняться через определенные промежутки времени, либо в случаях необходимости, когда система обнаружения вторжений (СОВ) будет сигнализировать о недостаточности применяемых мер защиты ИС и необходимости противодействия средствам ТКР (ПД ТКР). Помимо этого, динамичность структуры ИС будет достигаться автоматическим распределением динамических параметров новым абонентам ИС [3]. Однако, высокая частота смены сетевых параметров может отрицательно сказаться на стабильности активных критических соединений абонентов ИС.

Таким образом, стратегия клиент-серверной системы заключается в оценке достаточности применяемых мер защиты и оптимальным распределением сетевых параметров абонентам ИС, чего можно достичь верификацией результативности маскирования структуры ИС.

1. Постановка задачи

Приведенное описание процесса верификации результативности маскирования структуры информационной системы позволяет формализовать задачу исследования.

Формализуя задачу исследования сформулированы суть решаемой задачи, критерии ее решения, входные и выходные данные, важные факторы и условия задачи.

Для формальной постановки и решения задачи в исследовании введены нижеперечисленные обозначения.

Дано:

– S – клиент-серверная ИС;

– C – множество входных параметров ИС, включающих в себя запросы системы управления (СУ) на продление времени аренды и назначение сетевых параметров новым (вновь подключившимся) абонентам клиент-серверной (КС) ИС от DHCP-сервера «A», и воздействие ТКР «B»;

– Z – множество внутренних параметров модели, включает в себя S_i, Λ_j, где $S_i = \{S_1, S_2, \ldots, S_h\}$, $\Lambda_j = \{\lambda_1, \lambda_2, \ldots, \lambda_j\}$, перечень состояний системы и интенсивностей потоков событий в ней;

– P_i – множество выходных параметров модели, значения финальных вероятностей состояния системы S, $P_i = \lim\limits_{t \to \infty} P_i(t)$, где $i = 1, 2, \ldots, h$, причем число состояний конечно и из каждого из них можно за конечное число шагов перейти в любое другое;

– I – множество параметров условий функционирования, где I – протоколы транспортного уровня семейства протоколов TCP/IP, поддерживаемые моделируемой системой, I включает в себя протоколы TCP и UDP;

– Q – показатель эффективности маскирования логической структуры ИС, $Q = \lim\limits_{t \to \infty} P_D^C(t)$, $P_D^C(t) \to \min$, определяемый вскрытием ТКР логической структуры ИС.

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.

Тогда формальная постановка задачи на моделирование верификации результативности маскирования логической структуры ИС:

$$\mu :< S, C, Z, I > \rightarrow P_i, Q \mid C \subseteq (A, B), P_i = \lim_{t \to \infty} P_i(t) \qquad (1)$$

А формализованная постановка задачи на оптимизацию показателей эффективности верификации:

$$\begin{aligned} &< S, C, Z, I > \rightarrow \min P_D^C = \\ &= \lim_{t \to \infty} P_D^C(t) \mid P_D^C(t) \in \{P_i\}, i = 1, 2, \ldots, h \end{aligned} \qquad (2)$$

$$C \subseteq \{A, B\}; Z \subseteq \{S_i, \Lambda_j\}; I \subseteq \{TCP, UDP\}; Q = \lim_{t \to \infty} P_D^C(t) \qquad (3)$$

2. Модель верификации результативности маскирования структуры информационной системы

Разработка модели верификации результативности маскирования логической структуры ИС необходима для описания существенных свойств процессов верификации результативности маскирования ИС, что необходимо для разработки методики верификации результативности маскирования ИС.

Пусть имеется узел ИС – сервер, обеспечивающий функционирование клиент-серверной системы, в том числе и в части системы верификации результативности маскирования ИС. Моделируемая система S с течением времени меняет свое состояние (переходит из одного состояния в другое). Необходимые для исследования состояния клиент-серверной ИС можно отобразить как представлено в табл. 2.

Таблица 1

Дискретные состояния клиент-серверной ИС

Состояние	Описание состояния
S_1	Состояние покоя системы. Сетевые параметры абонентам ИС назначены и статичны. Воздействие средств ТКР отсутствует (или нейтрализованы)

Продолжение табл. 1

Состояние	Описание состояния
S_2	Изменение сетевых параметров абонентов КС ИС DHCP-сервером
S_3	Идентификация логической структуры ИС средствами ТКР в диалоговом режиме, средство ТКР осуществляет поочередное выполнение функций сетевого сканера
S_4	Логическая структура ИС вскрыта с некоторой полнотой, оценка результативности ТКР нарушителем
S_5	Обнаружение средств ТКР средствами СОВ
S_6	Оценка возможности изменить структурно-функциональные характеристики, оценка результативности защиты от средств ТКР

Моменты возможных переходов клиент-серверной ИС из состояния в состояние стохастичны и происходят в результате воздействия на систему потоков событий, характеризующиеся их интенсивностями λ, являющимися важной характеристикой потоков событий и характеризующими среднее число событий, приходящееся на единицу времени. Описания интенсивностей λ представлены в табл. 3.

Таблица 2

Интенсивности потоков событий в ИС

Интенсив-ность	Описание интенсивности потоков событий
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

Продолжение табл. 2

Интенсивность	Описание интенсивности потоков событий
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 ПД 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 ВН от DHCP-сервера в связи с недостаточностью результативности защиты от ТКР

Граф состояний [4] моделируемой клиент-серверной ИС представлен на рис. 1.

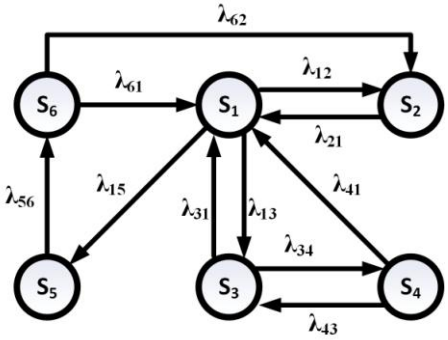


Рис. 1. Граф состояний верификации результативности маскирования структуры ИС

Оценка эффективности процессов верификации результативности маскирования логической структуры ИС связана с необходимостью моделирования процесса в реальном времени [5]. При этом:

– вероятность появления некоторого числа событий на любых непересекающихся промежутках времени зависит только от этого числа

событий и от длительности t промежутка и не зависит от начала его отсчета (свойство стационарности);

– считается, что появление двух и более событий за малый промежуток времени практически невозможно (свойство ординарности);

– появления того или иного количества событий в непересекающиеся промежутки времени взаимно независимы, (свойство отсутствия последствий).

Это обусловливает целесообразность использования математического аппарата марковских случайных процессов. Итак, процесс верификации результативности маскирования логической структуры ИС можно представить, как марковский случайный процесс с дискретными состояниями S_i и непрерывным временем dt.

По размеченному графу состояний процесса верификации результативности маскирования логической структуры ИС строится математическая модель ее функционирования – дифференциальные уравнения с неизвестными функциями $P_i(t)$.

$$\begin{cases} \dfrac{dp_1(t)}{dt} = \lambda_{61} p_6(t) + \lambda_{31} p_3(t) + \lambda_{41} p_4(t) + \lambda_{21} p_2(t) - \\ -\lambda_{12} p_1(t) - \lambda_{13} p_1(t) - \lambda_{15} p_1(t) \\ \dfrac{dp_2(t)}{dt} = \lambda_{12} p_1(t) + \lambda_{62} p_6(t) - \lambda_{21} p_2(t) \\ \dfrac{dp_3(t)}{dt} = \lambda_{13} p_1(t) + \lambda_{43} p_4(t) - \lambda_{31} p_3(t) - \lambda_{34} p_3(t) \\ \dfrac{dp_4(t)}{dt} = \lambda_{34} p_3(t) - \lambda_{43} p_4(t) - \lambda_{41} p_4(t) \\ \dfrac{dp_5(t)}{dt} = \lambda_{15} p_1(t) - \lambda_{56} p_5(t) \\ \dfrac{dp_6(t)}{dt} = \lambda_{56} p_5(t) - \lambda_{61} p_6(t) - \lambda_{62} p_6(t) \\ \sum_{i=1}^{6} p(t) = 1 \end{cases} \quad (4)$$

Используя известный порядок решения системы линейных дифференциальных уравнений методом Рунге-Кутты, учитывая вектор вероятностей начальных состояний $p_i(0)$, отрезок интегрирования $[t_0, t_1]$ и число этапов интегрирования n, произведен расчет для заданных значений интенсивностей событий $\lambda_{ij} = const$ (марковский однородный процесс), что позволило получить числовые таблицы приближенных значений p_i искомых решений $p(t)$ на некотором отрезке $t \in [t_0, t_1]$. Таким образом, получены вероятностные и временные характеристики, описывающие состояния процесса верификации результативности маскирования структуры ИС.

Оценим устойчивость модели к вариациям исходных данных, задавая граничные значения в стратегиях взаимодействующих сторон, при этом рассмотрим следующие сгенерированные последовательные состояния (стратегии):

– C_1 – с изменениями (штатными, протокольными) сетевых параметров и без попыток сканирования;

– C_2 – без заявок (штатных, протокольных) на изменение сетевых параметров и с попытками сканирования ТКР функционально-логической структуры (ФЛС) ИС (средства ТКР не обнаружены средствами СОВ);

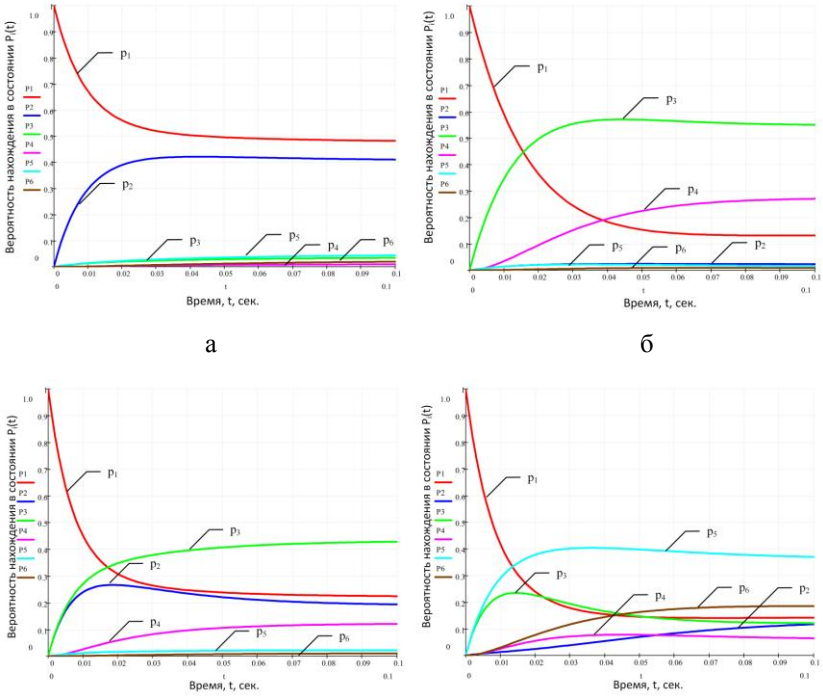
– C_3 – с изменениями (штатными, протокольными) сетевых параметров и с попытками сканирования ТКР ФЛС ИС (средства ТКР не обнаружены средствами СОВ);

– C_4 – без заявок (штатных, протокольных) на изменение сетевых параметров и с попытками сканирования ТКР ФЛС ИС (средства ТКР обнаружены средствами СОВ).

Графики зависимостей вероятностей состояний процесса верификации результативности маскирования структуры ИС от времени $p_1(t), p_2(t), ..., p_6(t)$, для значений интенсивностей событий, соответствующих стратегиям $C_1 - C_4$, представлены на рис. 2.

На отрезке времени $[0;0,1]$ ИС находится в переходном режиме функционирования, где наблюдается всплеск значений вероятности состояний. При $t \to \infty$ в ИС устанавливается стационарный режим, когда ИС случайным образом меняет свои состояния и ее вероятности

$p_1(t), p_2(t), \ldots, p_6(t)$ уже не зависят от времени и равны финальным (предельным) вероятностям.



а – стратегия C_1, *б – стратегия* C_1, *в – стратегия* C_1, *г – стратегия* C_1

Рис. 2. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий, соответствующих стратегиям $C_1 - C_4$

Заключение

Разработанная модель верификации результативности маскирования структуры ИС учитывает влияние и характер воздействия на ИС потоков событий на изменение сетевых параметров ИС, а также воздействия средств ТКР. Процесс защиты ИС в настоящей модели

заключается в минимизации вероятности потоков отказов средств СОВ и вскрытия ИС с требуемой ТКР полнотой. В связи с этим возникает необходимость поиска стратегий верификации результативности маскирования структуры ИС в зависимости от изменяющихся вариантов взаимодействия сторон из-за ограниченности ресурса сервера во времени. Модель позволяет вскрыть зависимости процесса верификации результативности маскирования структуры ИС от потоков воздействий, оценивать достаточность принятых мер защиты и обоснованно выбирать методики защиты ФЛС ИС.

Научная новизна модели заключается в применении математического аппарата теории марковских случайных процессов и решении уравнений Колмогорова для исследования и решения задачи верификации результативности маскирования структуры ИС путем оценки возможности изменить СФХ и оценки результативности защиты от средств ТКР.

Практическая значимость заключается в нахождении вероятностных и временных характеристик, описывающих состояния процесса верификации результативности маскирования структуры ИС при различных стратегиях изменений СФХ клиент-серверной ВС.

Список литературы

1. Инновационные информационные технологии в контексте обеспечения национальной безопасности государства / Р. В. Максимов [и др.] // Инновации. – 2018. – № 3 (233). – С. 28-35.

2. RFC 2131. Dynamic Host Configuration Protocol [Электронный ресурс] : база данных. – Режим доступа : https://www.protocols.ru/WP/rfc2131/

3. Максимов Р. В. Алгоритм и технические решения динамического конфигурирования клиент-серверных вычислительных сетей / Р. В. Максимов, С. П. Соколовский, И. С. Ворончихин // Цифровые информационно-телекоммуникационные технологии. – 2020. – Том 19 № 5. – С. 1090-1121.

4. Харари, Ф. Теория графов. Ф. Харари / Пер. с англ. и предисл. В. П. Козырева; Под ред. Г.П. Гаврилова – 2-е изд. – М. : УРСС, 2003. – 300 с.

5. Давыдов А. Е. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем : монография / А. Е. Давыдов, Р. В. Максимов, О. К. Савицкий. – М.: ОАО «Воентелеком», 2015. – 520 с.