МАСКИРОВАНИЕ МЕТАСТРУКТУР ИНФОРМАЦИОННЫХ СИСТЕМ В КИБЕРПРОСТРАНСТВЕ

Теленьга А.П.[1]

Цель исследования: *повышение защищенности информационных систем в киберпространстве от компьютерной разведки.*

Метод исследования: *методы математической статистики, нелинейной динамики, многокритериальной оптимизации.*

Результат исследования: *рассмотрены современные подходы к выделению уровней киберпространства, введено понятие метаструктуры информационной системы как протоколов и механизмов, которые обеспечивают интерфейс на различных уровнях киберпространства между базовыми компонентами системы, приложениями и сервисами, обслуживающими их, а также данными и информацией, сформулирована научная проблема маскирования метаструктур информационных систем в киберпространстве, заключающаяся в управления демаскирующими признаками метаструктур информационных систем: интенсивностью трафика между топологически локализованными сетевыми информационными объектами распределенной информационной системы, сетевыми протоколами взаимодействия и иерархическими уровнями (рангами) элементов информационной системы, постоянным перемещением между множественными конфигурациями информационной системы, на примере сетевого трафика поставлены непараметрическая и параметрическая задачи идентификации моделей метаструктур информационных систем.*

Научная новизна: *предложенная концепция отличается от известных выделением метаструктур информационных систем на различных уровнях киберпространства, постановкой задач маскировки, отравления, мимикрии и имитации информационной системы, управлением демаскирующими признаками метаструктур путем идентификации моделей информационных систем.*

Ключевые слова: *компьютерная разведка, компьютерная атака, сетевой трафик, идентификация модели, показатель Хёрста, динамическая трансформация временной шкалы, расстояние Кульбака-Лейблера.*

DOI:10.21681/4311-3456-2023-5-50-59

Введение

Рядом авторов, как зарубежных, так и отечественных [1-4], вводится понятие киберпространства как искусственного неоднородного технологического пространства со множеством разноуровневых органов оперативного и технологического управления, процесс создания и эксплуатации которого не предопределяется требованиями одной системы управления, а функционирует в интересах множества разнородных, в том числе антагонистических, систем управления, при этом его свойства зависят как от характеристик собственных элементов, так и от объема и свойств реализуемых процессов в интересах внутренних и внешних потребителей.

В соответствии с данным определением, информационные системы (далее – ИС), функционирующие в киберпространстве, представляют собой совокупность территориально распределенных сегментов, объединенных каналами связи различной протяженности с использованием коммуникационных технологий (оборудования) через сети связи общего пользования (ССОП) с целью предоставления пользователям информационных систем информационных ресурсов (программ и сервисов).

Формирование структуры ИС не происходит одномоментно. Она изменяется в ходе повседневной деятельности, внештатных ситуаций или преднамеренного информационно-технического воздействия. Образно говоря, ИС «мерцает» во времени, поэтому традиционное представление в виде двух- или трехмерных конструкций (граф, матрица связности) даёт возможность наблюдать лишь «срезы» ИС, причём в различные моменты времени наблюдаются их различные проявления.

1 Теленьга Александр Павлович, кандидат педагогических наук, докторант Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: alexander.telenga@yandex.ru, ORCID: 0000-0001-6193-0656

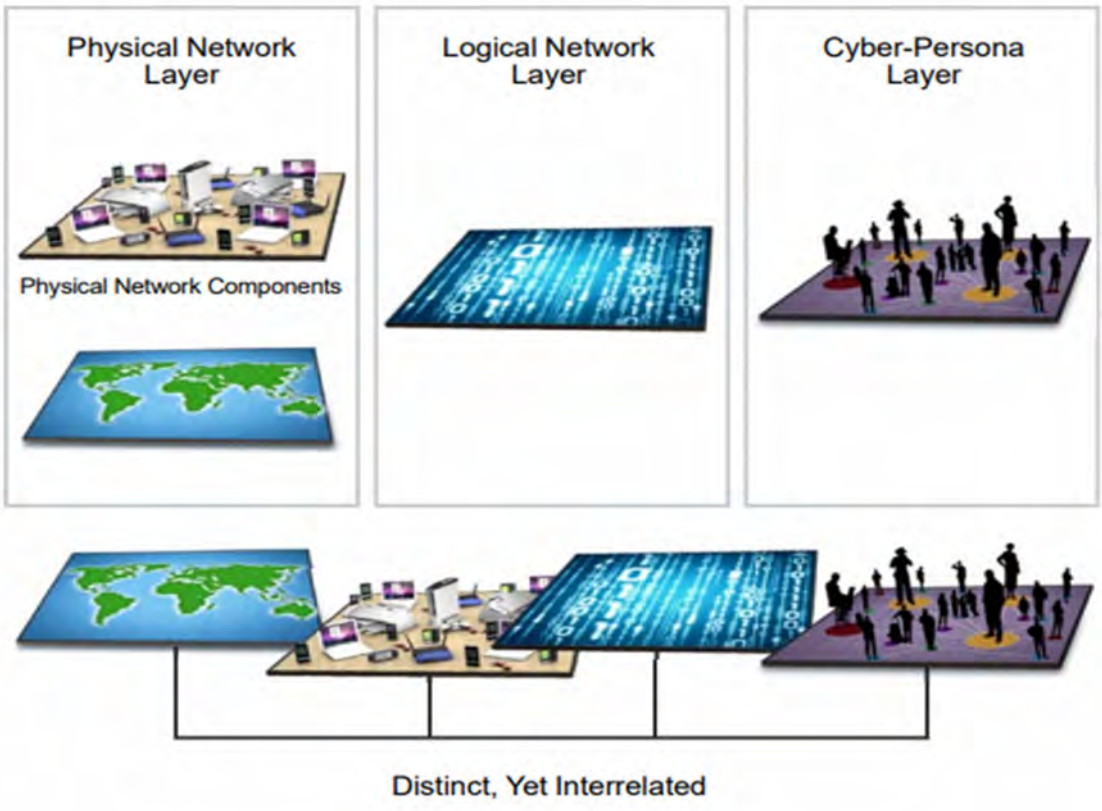

Рис. 1. Три взаимосвязанных уровня киберпространства согласно концепции Киберкомандования США

Согласно концепции Киберкомандования США [5] (рис. 1), в киберпространстве выделяются следующие уровни: кибер-идентификации, логической сети и физической сети.

Исходя из этого, логическая модель информационной системы в терминах структур позволяет выделить следующие уровни (рис. 2):

1. **Инфраструктура** – базовые компоненты системы: вычислительные мощности, сеть и хранилище данных.
2. **Апплиструктура** – приложения информационной системы и сервисы, обслуживающие их.
3. **Инфоструктура** – данные и информация. Содержимое баз данных, файловых хранилищ и т.д..
4. **Метаструктура** – протоколы и механизмы, которые обеспечивают интерфейс между инфраструктурой, структурой приложений и структурой данных в информационной системе, закон группы, которую образуют разнородные структуры.

Подобно «вторичным структурам» в геологии, возникающим в горной породе под влиянием позднейших процессов, например, механического, термального или химического воздействия, можно говорить о формировании в киберпространстве метаструктур ИС, которые могут обнаруживаться как информационные следы на соответствующем уровне киберпространства. Так, примером статистического следа на уровне логической сети является сетевой трафик ИС, семантического следа на уровне кибер-идентификации – служебная информация операционных систем, приложений, а структурный след на уровне физической сети проявляется в перколяционных процессах кластеров сетей передачи данных.

Предпосылки к идентификации моделей метаструктур информационных систем

В настоящее время киберпространство продолжает развиваться и усложняться. В связи с этим необходимо глубокое научное понимание закономерностей и тенденций этого развития. Требует в том числе внимания проблема информационно-технологического противоборства, методов ведения оборонительных, наступательных и разведывательных операций в киберпространстве, проблемы обеспечения надежного сдерживания в этой области.

Конфликты в киберпространстве характеризуются тем, что все его участники имеют развитые системы мониторинга и наблюдения состояния антагониста,

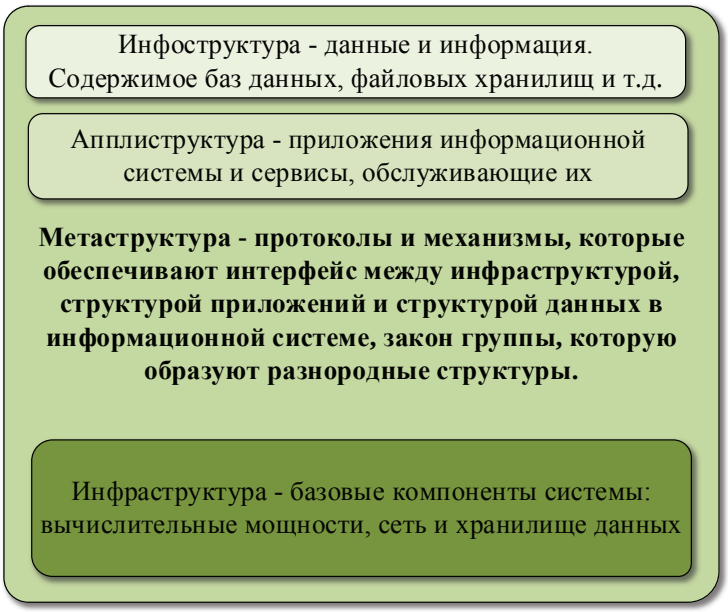

Рис. 2. Модель ИС в терминах структур

Рис. 3. Техники компьютерной разведки

системы информационного воздействия, а также собственные защищаемые информационно-управляющие системы.

Статичность, однородность и детерминированность, определяющие постоянство состава, структуры и алгоритмов функционирования ИС, обуславливают наличие у злоумышленника ряда преимуществ в использовании временного и вычислительного ресурса для ведения компьютерной разведки (КР), обеспечивающих ему:

— возможность с небольшими ресурсными затратами проводить крупномасштабную атаку после успешного проведения мелкомасштабной атаки;
— высокую достоверность результатов КР в течение длительного времени, что позволяет осуществлять планирование, выбор времени и технологического процесса ИС для начала компьютерных атак (КА);
— возможность бескомпроматного применения средств КР и реализации КА, в любое удобное для этого время, за счет заблаговременного (планового) формирования и применения их оптимального набора;
— возможность неоднократного обнаружения и анализа уязвимостей аппаратного и программного обеспечения, с последующим их тестированием на проникновение для конкретной цели и т.д.

Согласно методологии описания этапов компьютерной атаки *Cyber KillChain*, разработанной компанией *Lockheed Matrin* [6], любая атака начинается с разведки. База знаний тактик и техник злоумышленников *MITRE ATT&CK* выделяет 10 групп техник разведки (рис. 3).

Разнообразие этих техник и их комбинаций на различных уровнях киберпространства, а также возможность анализа полученной информации методами

глубокого анализа данных, существенно повышает вероятность обнаружения вскрытия структуры ИС через выявленные метаструктуры, а значит, и осуществления вредоносного воздействия.

В настоящее время в состав мер защиты информации в государственных информационных системах включены:

— сокрытие архитектуры и конфигурации ИС;
— создание (эмуляция) ложных ИС или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации;
— воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик ИС или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках ИС.

Это вызвано тем, что достаточно большое количество КА выполняется средствами КР с целью получения информации о составе, структуре и алгоритмах функционирования, местоположении и принадлежности ИС, а также данных, хранимых, обрабатываемых и передаваемых в таких ИС. Наряду с угрозами безопасности информации, связанными с диалоговым взаимодействием нарушителя и ИС (в частности – автоматизированными средствами сетевого сканирования), на реконструкцию структурно-функциональных характеристик ИС нацелена угроза определения топологии ИС, бескомпроматно реализуемая анализом сетевого трафика. Результат – вскрытие топологии распределенной в киберпространстве ИС, определение важности ее узлов – может быть использован нарушителем для реализации спланированных *APT*-атак (от англ. *advanced persistent threat* – «развитая устойчивая угроза», целевая кибератака).

Задача реализации перечисленных выше мер защиты информации может быть решена маскированием метаструктур ИС [7] – совокупностью ложных (маскирующих) техник, выполняемых сетевыми информационными объектами (СИО) с целью управления демаскирующими признаками (ДМП) метаструктур ИС: интенсивностью трафика между топологически локализованными СИО распределенной ИС, сетевыми протоколами взаимодействия и иерархическими уровнями (рангами) элементов ИС, постоянным перемещением между множественными конфигурациями ИС, что увеличивает неопределенность данных у КР и лишает её возможности ретроспективного анализа данных разведки.

Обстановка в разных условиях функционирования ИС требует решения следующих задач маскирования [8-10]:

1. Необходимо дополнить метаструктуры ИС до метаструктур ССОП, иными словами, необходима *маскировка* метаструктур ИС под метаструктуры ССОП, поскольку разнообразие уникальных цифровых отпечатков устройств ИС – набора параметров, позволяющих однозначно идентифицировать устройство пользователя –несоизмеримо меньше, чем устройств ССОП.
2. Необходимо *«отравить» (насытить)* метаструктуру ИС ложными данными для снижения эффективности средств КР. В этом случае применение злоумышленником, например, методов глубокого анализа данных для ведения КР будет существенно затруднено.
3. Необходимо *имитировать* метаструктуру ИС для обеспечения успешного киберманеврирования. Сущность киберманевра заключается в искусственном расширении поверхности атаки за счёт создания ложных целей.
4. Необходима *мимикрия* метаструктур ССОП под метаструктуры ИС с целью введения в заблуждение средств КР и отвлечения внимания.

При этом перечисленные выше задачи могут решаться как по отдельности, так и совместно, образуя комплекс средств маскирования.

Очевидно, что для успешного решения поставленных задач необходимо вскрыть закономерности изменения метаструктур ИС во времени, проведя реконструкцию динамических моделей (такой термин принят в нелинейной динамике), или идентификацию систем (в терминах математической статистики), т.е. определение структуры и параметров (параметрическая идентификация) или наилучшей аппроксимации характеристик (непараметрическая идентификация) по полученному экспериментальному набору данных (записанных входных и выходных сигналов) [11-13]. Математическая модель метаструктур ИС в этом случае задаётся в виде уравнений, описывающих связь одной или нескольких случайных переменных с другими переменными (случайными и детерминистическими).

Задача непараметрической идентификации модели метаструктур информационных систем

Особенностью методов непараметрической идентификации (получение описания одной или нескольких случайных переменных модели) является то, что в них либо не учитывается закон распределения полученных

данных, либо учитывается с неявно определенными параметрами. Другими словами, в методах непараметрического идентификации статистическая модель (и ее структура) не имеет фиксированного числа параметров.

К таковым относятся:

— построение графика функции плотности распределения вероятности (например, гистограммой);
— ядерная оценка (сглаживание) плотности распределения (под ядром понимается некоторая весовая функция);
— непараметрическая регрессия (на базе ядер, сплайнов, вейвлетов и др.);
— ряд методов классификации и кластеризации (например, kNN, SVM);
— проверка статистических гипотез.

Построение графика функции плотности распределения вероятности гистограммой проводится следующим образом. Для набора из N случайных переменных $\{X_1, X_2, ..., X_N\}$ количество c_i попаданий X_j в i-ый подинтервал $[a_{i-1}, a_i]$ исходного интервала $[a_0, a_n]$ для $i = 1, 2, ..., n$ (теоретически, $[-\infty, +\infty]$) определяется как

$$c_i = \sum_{j=1}^{N} \{1 : X_j \in [a_{i-1}, a_i]\} \quad (1)$$

Тогда кусочнопостоянная функция $h(x)$, называемая нормализованной гистограммой, оценивается следующим образом:

$$h(x) = \frac{c_i}{N\Delta a_i} = \frac{c_i}{N(a_i - a_{i-1})}. \quad (2)$$

Нормализованная гистограмма есть графическая интерпретация функции плотности распределения вероятности.

Кроме нормализованной гистограммы используется интегральная гистограмма. Для набора из N случайных переменных $\{X_1, X_2, ..., X_N\}$ количество c_i попаданий X_j в i-ый подинтервал $[a_0, a_i]$ исходного интервала $[a_0, a_n]$ для $i = 1, 2, ..., n$ (теоретически, $[-\infty, +\infty]$) определяется как:

$$c_i = \sum_{j=1}^{N} \{1 : X_j \in [a_0, a_i]\} \quad (3)$$

Нормализованная интегральная гистограмма $h(x)$, являющаяся функцией распределения вероятности, оценивается следующим образом:

$$h^{инт}(x) = \frac{c_i}{N\Delta a_i} = \frac{c_i}{N(a_i - a_0)}. \quad (4)$$

Другим видом непараметрической идентификации является ядерная оценка плотности или ядерное сглаживание (kernel density estimation). Для набора из N случайных переменных $\{X_1, X_2, ..., X_N\}$ форма (огибающая) функции плотности распределения вероятности определяется как

$$f_{KDE}(x) = \frac{1}{N}\sum_{j=1}^{N} K_h(x - X_j) = \frac{1}{Nb}\sum_{j=1}^{N} K_h\left(\frac{x - X_j}{b}\right) \quad (5)$$

где $K(\cdot)$ – ядро, неотрицательная функция, интегрируемая в 1, $b > 0$ – параметр сглаживания.

Проверка статистических гипотез направлена на численное принятие решения о том, удовлетворяет ли статистическая выборка заданной статистической гипотезе. С практической точки зрения, как правило, речь идёт о следующем:

— описывается ли случайная переменная из имеющейся выборки заданным законом распределения;
— принадлежат ли две случайные величины из имеющейся выборки к одному закону распределения.

Задача параметрической идентификации модели метаструктур информационных систем

В случае параметрической идентификации под моделью метаструктуры ИС будем понимать отображение структуры S и параметров X в свойства Y:

$$Y = F(S, X_S). \quad (6)$$

Пусть $\mathbf{Y}^{треб}$ – вектор требуемых свойств метаструктуры ИС. Тогда задача идентификации модели заключается в определении множества структур Ω_S и параметров $\Omega_X : \mathbf{Y}^{треб} = F(S, X_S), S \in \Omega_S, X_S \in \Omega_X(S)$.

Задача сводится к экстремальной задаче

$$\left|\mathbf{Y}^{треб} - F(S, X_S)\right| \to \min_{S, X_S}. \quad (7)$$

Все возможные результаты решения экстремальной задачи образуют множества Ω_S и Ω_X.

На стадии оптимизации производится синтез оптимальной конструкции из допустимого множества структур и параметров. Для этого прежде всего необходимо задать критерии оптимальности. Эти критерии могут быть трех типов:

а) типа неравенств:

$H(S, X_S) \geq 0$ или $h_i(S, X_S) \geq 0, i = 1, ..., m$, где $H = (h_1, h_2, ..., h_m)$;

б) типа равенств:

$G(S, X_S) = 0$ или $g_i(S, X_S) = 0, i = 1, ..., p$, где $G = (g_1, g_2, ..., g_p)$;

в) экстремального типа:

$Q(S, X_S) \to extr$ или $q_i(S, X_S) \to 0, i = 1, ..., k$, где $Q = (q_1, q_2, ..., q_k)$, т. е. экстремальная задача имеет многокритериальный характер.

Вид критериев H, G и Q определяется, исходя из технологических, эксплуатационных и других соображений. В общем виде задача оптимальной идентификации моделей метаструктур информационных формулируется в виде

$$Q(S, X_S) \to \underset{S, X_S \in \Psi}{extr}, \quad (8)$$

где

$$\Psi = \begin{cases} H(S, X_S) \geq 0, \\ G(S, X_S) = 0, \\ S \in \Omega_S, \\ X_S \in \Omega_X(S) \end{cases}. \quad (9)$$

Постановка задачи идентификации модели сетевого трафика

Рассмотрим в качестве метаструктуры, модель которой необходимо идентифицировать, сетевой трафик ИС.

Существует несколько подходов к описанию сетевого трафика ИС: в виде потоков и в виде последовательности пакетов («сырой» трафик).

Потоки содержат заголовочную информацию о сетевых соединениях между двумя конечными устройствами, такими как серверы или рабочие станции. Каждый поток представляет собой совокупность переданных сетевых пакетов, которые имеют некоторые общие свойства. Как правило, все передаваемые сетевые пакеты с одинаковыми IP-адресом источника, портом источника, *IP*-адресом назначения, порт назначения и транспортным протоколом в пределах временного окна объединяются в один поток [14, 15].

«Сырой» трафик, как правило, представляет собой последовательность пакетов, каждый из которых содержит время отправки пакета, *IP*-адрес источника, порт источника, IP-адрес назначения, порт назначения, протокол, размер пакета, установленные флаги и поле данных, в которое записывается полезная нагрузка [16, 17].

Известно, что сетевой трафик обладает свойством самоподобия его статистических свойств в *IP*-сетях не только в текущий момент времени, но и ретроспективно. Это означает, что присутствует повторяемость статистических характеристик естественных временных рядов с изменением масштаба. Процессы, обладающие свойствами самоподобия, характеризуются наличием последействия за счет факторов, вызывающих сложные зависимости: при относительно низкой средней скорости поступления пакетов сообщений возможны большие всплески интенсивности [18]. Статистические характеристики такого процесса – ДМП конкретной информационной системы.

Общепринятым показателем самоподобия процесса является показатель Хёрста H, в зависимости от значений которого делают следующие выводы об исследуемых процессах: при $0 \leq H \leq 0,5$ случайный процесс не обладает самоподобием; при $H > 0,5$ – процесс обладает длительной памятью и является самоподобным.

Таким образом, разность между показателем Хёрста эталонного и модельного трафика может выступать в качестве метрики близости модели и реального сетевого трафика:

$$q_1(S, X_S) = \left| H_{ориг} - H_{модель} \right| \to \min. \quad (10)$$

Ещё одним критерием выступает динамическая трансформация временной шкалы *Dynamic time warping* (*DTW*) – это метод анализа временных рядов, который позволяет сравнивать и выявлять сходства между двумя временными рядами, имеющими различную скорость изменения [19]. Он основан на алгоритме динамического программирования, который вычисляет оптимальное выравнивание между двумя временными рядами, учитывая возможные различия в скорости изменения.

$$q_2(S, X_S) = \left| DTW(Y^{треб}, F(S, X_s)) \right| \to \min. \quad (11)$$

Формальная постановка непараметрической идентификации модели времени задержек между пакетами сетевого трафика формулируется следующим образом: необходимо обеспечить минимальность разности между показателями самоподобия исходного и модельного временных рядов (10), а также минимальность динамической трансформации временной шкалы (11) в соответствующей метрике при заданном допустимом множестве структур S и параметров X_S:

$$\Psi = \begin{cases} H_{модель} \geq 0,5, \\ q_1(S, X_S) \leq 10^{-3}, \\ q_2(S, X_S) \leq 10, \\ S \in \{S_1, S_2, S_3, S_4, S_5\}, \\ X_s \in \{X_{S_1}, X_{S_2}, X_{S_3}, X_{S_4}, X_{S_5}\} \\ S_1 = f(X_{S_1}), S_2 = f(X_{S_2}), S_3 = f(X_{S_3}), \\ S_4 = f(X_{S_4}), S_5 = f(X_{S_5}) \\ X_{S_1} = \{N_{KN}, b_{KN}\}, X_{S_2} = \{N_{KE}, b_{KE}\}, X_{S_3} = \{A, B\}, \\ X_{S_4} = \{\mu_{LN}, \sigma_{LN}\}, X_{S_5} = \{\mu_{HN}, \sigma_{HN}\}, \\ b_{KN} > 0, b_{KE} > 0, A > 0, B > 0, \sigma_{LN} \geq 0, \ \sigma_{HN} \geq 0 \end{cases}. \quad (12)$$

S – тип модельного оператора.

X_S – параметры модельного оператора.

Прямое решение задачи векторной оптимизации представляет собой множество параметров, оптимальных по Парето. Исходя из равнозначности критериев, характера достижимого критериального пространства и поставленной цели исследования, выбор одного оптимального набора типа и параметров модельного оператора целесообразно осуществлять с использованием метода идеальной точки. За «идеальную точку» принимаются экстремальные (идеальные) значения целевых функций $q_i(S, X_S)$.

Тогда скалярная целевая функция $R(S, X_S)$ имеет физический смысл евклидовой метрики (расстояния) между «идеальной точкой» и точкой фронта Парето, а выбор оптимального набора значений исходных целевых функций и факторов аргументов соответствует минимальному значению указанного расстояния, тогда скалярная целевая функция имеет вид:

$$\begin{cases} R = \sqrt{(q_1(S, X_S) - 0)^2 + (q_2(S, X_S) - 0)^2} \\ R \to \min\limits_{S, X_S \in \Psi} \end{cases}, \quad (13)$$

где (0,0) – координаты идеальной точки в критериальном пространстве $q_1(S, X_S) \times q_2(S, X_S)$.

Исходя из характера исследуемых процессов, в качестве модельных операторов могут использоваться следующие.

— Гауссово ядро:

$$S_1 = f(x \mid N, b) = \frac{1}{\sqrt{2\pi} Nb} \sum_{j=1}^{N} e^{-\frac{1}{2}\left(\frac{x - X_j}{b}\right)^2} \quad (14)$$

— Епанечниково ядро:

$$S_2 = f(x \mid N, b) = \frac{3}{4Nb} \sum_{j=1}^{N} \left(1 - \left(\frac{x - X_j}{b}\right)^2\right), |x| < 1 \quad (15)$$

— Функции плотностей распределений Вейбула, логнормального и полунормального соответственно:

$$S_3 = f(x \mid a, b) = \begin{cases} \frac{b}{a}\left(\frac{x}{a}\right)^{b-1} e^{-(x/a)^b}, x \geq 0 \\ 0, x < 0 \end{cases} \quad (16)$$

$$S_4 = f(x \mid \mu, \sigma) = \frac{1}{x\sigma\sqrt{2\pi}} exp\left\{\frac{-(\log x - \mu)^2}{2\sigma^2}\right\}, x > 0 \quad (17)$$

$$S_5 = f(x \mid \mu, \sigma) = \sqrt{\frac{2}{\pi}} \frac{1}{\sigma} e^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2}, x \geq \mu \quad (18)$$

Динамическая трансформация временной шкалы DTW использует метрику расстояния между временными рядами. Поскольку непараметрическая идентификация подразумевает вероятностный характер моделей, в качестве метрики выбрана симметричная дивергенция Кульбака-Лейблера [20].

$$d_{mn}(\mathbf{X}, \mathbf{Y}) = \sum_{k=1}^{K} (x_{k,m} - y_{k,n})(\log x_{k,m} - \log y_{k,n}) \quad (19)$$

Формальная постановка параметрической идентификации модели времени задержек между пакетами сетевого трафика формулируется следующим образом: необходимо обеспечить минимальность разности между показателями самоподобия исходного и модельного временных рядов (10), а также минимальность динамической трансформации временной шкалы (11) в метрике евклидового расстояния при множестве допустимых параметров

$$\Psi = \begin{cases} H_{модель} \geq 0,5, \\ q_1(S, X_S) \leq 10^{-3}, \\ q_2(S, X_S) \leq 30, \\ S \in \{S_1, S_2, S_3\}, \\ X_s \in \{X_{S_1}, X_{S_2}, X_{S_3}\}, \\ S_1 = f(X_{S_1}), S_2 = f(X_{S_2}), S_3 = f(X_{S_3}), \\ X_{S_1} = \{A, B\}, X_{S_2} = \{\sigma, \rho, \beta\}, X_{S_3} = \{a, b, \tau\}, \\ 0 < A \leq 50, 0 < B \leq 50, 0 < \sigma \leq 20, 0 < \beta \leq 20, \\ 0 < \rho \leq 17, 0 < a \leq 20, 0 < b \leq 20, 0 < \tau \leq 17 \end{cases} \quad (20)$$

При этом в качестве метрики расстояния между рядами для DTW может быть выбрано евклидово расстояние:

$$d_{mn}(\mathbf{X}, \mathbf{Y}) = \sqrt{\sum_{k=1}^{K} (x_{k,m} - y_{k,n})(x_{k,m} - y_{k,n})} \quad (21)$$

В качестве модельных операторов используются динамические системы, известные самоподобным поведением [21].

— Уравнение нелинейного осциллятора Ван дер Поля

$$S_1 = f(x \mid A, B) = \frac{d^2x}{d^2t} - A(1 - B\frac{dx}{dt}) + x = 0. \quad (22)$$

— Уравнение Лоренца

$$S_2 = f(x, y, z \mid \sigma, \rho, \beta) = \begin{cases} \frac{dx}{dt} = \sigma(y - x) \\ \frac{dy}{dt} = x(\rho - z) - y \\ \frac{dz}{dt} = xy - \beta z \end{cases} \quad (23)$$

— Уравнение генератора Мэки-Гласса

$$S_3 = f(x \mid a,b,\tau) = \frac{dx(t)}{dt} - \frac{ax(t-\tau)}{1+x(t-\tau)^{10}} + bx(t) = 0 \quad (24)$$

Получившаяся задача векторной оптимизации также может быть сведена к скалярной методом идеальной точки (13).

Выводы

Анализ современных подходов к выделению уровней киберпространства позволяет утверждать, что функционирование антагонистических систем происходит на уровне кибер-идентификации, логической сети и физической сети. Предложенное понятие метаструктуры информационной системы, имманентное её информационным следам, может быть определено как протоколы и механизмы, которые обеспечивают интерфейс на различных уровнях киберпространства между базовыми компонентами системы, приложениями и сервисами, обслуживающими их, а также данными и информацией.

Статичность, однородность и детерминированность, определяющие постоянство состава, структуры и алгоритмов функционирования информационных систем обуславливают наличие у злоумышленника ряда преимуществ в использовании временного и вычислительного ресурса для ведения компьютерной разведки, в связи с чем сформулирована научная проблема маскирования метаструктур информационных систем в киберпространстве, заключающаяся в управления демаскирующими признаками метаструктур информационных систем: интенсивностью трафика между топологически локализованными сетевыми информационными объектами распределенной информационной системы, сетевыми протоколами взаимодействия и иерархическими уровнями (рангами) элементов информационной системы, постоянным перемещением между множественными конфигурациями информационной системы.

Решение указанных задач невозможно без вскрытия закономерностей изменения метаструктур информационных систем во времени, для чего необходимо провести идентификацию их моделей или реконструкцию динамических систем, описывающих процесс функционирования информационных систем. На примере сетевого трафика поставлены непараметрическая и параметрическая задачи идентификации моделей метаструктур информационных систем, определены критерии оптимальности и сформулирована экстремальная задача выбора оптимальных параметров модели.

Таким образом, в условиях ведения злоумышленником компьютерной разведки и реализации компьютерных атак выделение метаструктур ИС, идентификация их моделей и маскирование методами введения в заблуждение и повышения неопределенности позволит обеспечить гибкость, адаптивность и повысит эффективность системы защиты.

Научный консультант: Максимов Роман Викторович, доктор технических наук, профессор, профессор Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменное училища имени генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: rvmaxim@yandex.ru

Литература

1. Стародубцев, Ю. И. Техносферная война как основной способ разрешения конфликтов в условиях глобализации / Ю. И. Стародубцев, П. В. Закалкин, С. А. Иванов. // Военная Мысль. — 2020. — № 10. — С. 16-21.
2. Стародубцев, Ю. И. Концептуальные направления решения проблемы обеспечения устойчивости Единой сети электросвязи Российской Федерации / Ю. И. Стародубцев, С. А. Иванов, П. В. Закалкин. // Военная Мысль. — 2021. — № 4. — С. 39-49.
3. Zdzikot, T. Cyberspace and Cybersecurity / T. Zdzikot. // Cybersecurity in Poland. — Cham: Springer, 2022. — С. 9-21. DOI 10.1007/978-3-030-78551-2_2
4. Theoretical basis and technical methods of cyberspace geography / Gao Chundong, Guo Qiquan, Jiang Dong [и др.]. // Journal of Geographical Sciences. — 2019. — № 29. — С. 1949–1964.
5. Joint Chiefs of Staff. Cyberspace operations. Joint Chiefs of Staff (US); 19 2022 Dec 19. Joint Publication No.: JP 3-12. // Official Website of the Joint Chiefs of Staff: [сайт]. — URL: https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/ (дата обращения: 26.08.2023).
6. Lockheed Martin's Cyber-Kill Chain. // Leading Aerospace and Defense | Lockheed Martin: [сайт]. — URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (дата обращения: 26.08.2023).
7. Теленьга А.П. Анализ возможностей обнаружения метаструктур информационных систем специального назначения. / А. П. Теленьга // Кибербезопасность: угрозы, тенденции, технологии защиты: материалы II Межведомственной науч.-практич. конф., 19-20 мая 2022 г. / Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М.Штеменко. – Краснодар: КВВУ, 2022. С.70-76
8. Zheng, Y. Dynamic defenses in cyber security: Techniques, methods and challenges / Y. Zheng, Z. Li, X. Xu // Digital Communications and Networks. — 2022. — № 8. — С. 422–435.

9. Shaping Attacker Behavior: Evaluation of an Enhanced Cyber Maneuver Framework / J. A. McKneely, T. K. Sell, K. A. Straub [и др.] // HCII 2022: HCI for Cybersecurity, Privacy and Trust. — Cham: Springer, 2022. — С. 358–379. – DOI: 10.1007/978-3-031-05563-8_23
10. Lilli, E. How Can We Know What We Think We Know about Cyber Operations? / E. Lilli // Journal of Global Security Studies. — 2023. — № 8(2). — С. 1–18. – DOI 10.1093/jogss/ogad011
11. Dynamic-chaos information technologies for data transmission, storage, and protection / Yu. V. Gulyaev, R. V. Belyaev, G. M. Vorontsov [et al.] // Радиоэлектроника. Наносистемы. Информационные технологии. – 2018. – Vol. 10, No. 2. – P. 279-312. – DOI 10.17725/rensit.2018.10.279.
12. Четвертакова, Ю. С. Построение моделей стохастических нелинейных динамических систем на основе двухэтапной процедуры параметрической идентификации / Ю. С. Четвертакова, О. С. Черникова // Наука. Технологии. Инновации: Сборник научных трудов. В 9-ти частях, Новосибирск, 30 ноября – 04 2020 года / Под редакцией А.В. Гадюкиной. Том Часть 2. – Новосибирск: Новосибирский государственный технический университет, 2020. – С. 94-98.
13. Карганов, В. В. К вопросу о необходимости моделирования информационных систем организации, функционирующих в условиях угроз безопасности / В. В. Карганов // Национальная безопасность России: актуальные аспекты : Сборник статей Всероссийской научно-практической конференции, Санкт-Петербург, 30 июля 2019 года. – Санкт-Петербург: Частное научно-образовательное учреждение дополнительного профессионального образования Гуманитарный национальный исследовательский институт «НАЦ-РАЗВИТИЕ», 2019. – С. 20-30.
14. Будко, Н. П. Общие принципы функционирования и требования к построению структур перспективных систем мониторинга распределенных информационно-телекоммуникационных сетей / Н. П. Будко // Техника средств связи. – 2021. – № 2(154). – С. 38-59.
15. Голованов, А. А. Сравнительный анализ систем обнаружений аномалий с использованием потока сетевого трафика и протокола NETFLOW / А. А. Голованов, О. И. Мельникова // Международный научно-исследовательский журнал. – 2023. – № 6(132). – DOI 10.23670/IRJ.2023.132.18.
16. Полтавцева, М. А. Формирование структур данных в задачах активного мониторинга безопасности // Проблемы информационной безопасности. Компьютерные системы. – 2021. – № 1. – С. 9-19.
17. Alothman, B., Raw Network Traffic Data Preprocessing and Preparation for Automatic Analysis // 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). – 2019. – P. 1-5, DOI: 10.1109/CyberSecPODS.2019.8885333.
18. Черниговский, А. В. Оценка степени самоподобия сетевого трафика / А. В. Черниговский, М. В. Кривов // Информационные технологии. Проблемы и решения. – 2019. – № 1(6). – С. 115-120.
19. Chen, L. A deep multi-task representation learning method for time series classification and retrieval / L. Chen, D. Chen, F. Yang, J. Sun // Information Sciences. – 2021. – Vol. 555. – P. 17-32. – DOI 10.1016/j.ins.2020.12.062.
20. Калинин, М. Ю. Энтропийные оценки решающих статистик алгоритма классификации случайных процессов / М. Ю. Калинин, О. Н. Чопоров // Моделирование, оптимизация и информационные технологии. – 2020. – Т. 8, № 4(31). – DOI 10.26102/2310-6018/2020.31.4.034.
21. Соколовский, С. П. Методика формирования ложного сетевого трафика информационных систем для защиты от сетевой разведки / С. П. Соколовский, А. П. Теленьга // Вестник компьютерных и информационных технологий. – 2022. – Т. 19, № 2(212). – С. 40-47. – DOI: 10.14489/vkit.2022.02.pp.040-047.

MASKING METASRTRUCTURES OF INFORMATION SYSTEMS IN CYBERSPACE

***Telenga A.P.*[2]**

Research objective: *to improve the security of information systems in cyberspace against computer reconnaissance.*

Research method: *methods of mathematical statistics, nonlinear dynamics, multicriteria optimization.*

Research results: *modern approaches to the allocation of cyberspace levels are considered, the concept of information system metastructure is introduced as protocols and mechanisms that provide an interface at different levels of cyberspace between the basic components of the system, applications and services that serve them, as well as data and information, the scientific problem of masking metastructures of information systems in cyberspace is formulated, which consists in the management of demasking features of metastructures of information systems in cyberspace.*

Scientific novelty: *the proposed concept differs from the known ones by singling out metastructures of information systems at different levels of cyberspace, setting tasks of masking, poisoning, mimicry and imitation of information systems, management of demasking features of metastructures by identifying models of information systems.*

Keywords: *computer reconnaissance, computer attack, network traffic, model identification, Hurst index, dynamic time warping, Kulbak-Leibler distance.*

2 Telenga Alexander Pavlovich, candidate of pedagogical sciences, Doctoral student, Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, E-mail: alexander.telenga@yandex.ru, ORCID: 0000-0001-6193-0656

References

1. Starodubcev, Yu. I. Texnosfernaya vojna kak osnovnoj sposob razresheniya konfliktov v usloviyax globalizacii / Yu. I. Starodubcev, P. V. Zakalkin, S. A. Ivanov. // Voennaya My`sl`. — 2020. — № 10. — S. 16-21.
2. Starodubcev, Yu. I. Konceptual`ny`e napravleniya resheniya problemy` obespecheniya ustojchivosti Edinoj seti e`lektrosvyazi Rossijskoj Federacii / Yu. I. Starodubcev, S. A. Ivanov, P. V. Zakalkin. // Voennaya My`sl`. — 2021. — № 4. — S. 39-49.
3. Zdzikot, T. Cyberspace and Cybersecurity / T. Zdzikot. // Cybersecurity in Poland. — Cham: Springer, 2022. — S. 9-21. DOI 10.1007/978-3-030-78551-2_2
4. Theoretical basis and technical methods of cyberspace geography / Gao Chundong, Guo Qiquan, Jiang Dong [i dr.]. // Journal of Geographical Sciences. — 2019. — № 29. — S. 1949–1964.
5. Joint Chiefs of Staff. Cyberspace operations. Joint Chiefs of Staff (US); 19 2022 Dec 19. Joint Publication No.: JP 3-12. // Official Website of the Joint Chiefs of Staff: [sajt]. — URL: https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/ (data obrashheniya: 26.08.2023).
6. Lockheed Martin's Cyber-Kill Chain. // Leading Aerospace and Defense | Lockheed Martin: [sajt]. — URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (data obrashheniya: 26.08.2023).
7. Telen`ga A.P. Analiz vozmozhnostej obnaruzheniya metastruktur informacionny`x sistem special`nogo naznacheniya. / A. P. Telen`ga // Kiberbezopasnost`: ugrozy`, tendencii, texnologii zashhity`: materialy` II Mezhvedomstvennoj nauch.-praktich. konf., 19-20 maya 2022 g. / Krasnodarskoe vy`sshee voennoe ordenov Zhukova i Oktyabr`skoj Revolyucii Krasnoznamennoe uchilishhe imeni generala armii S.M.Shtemenko. – Krasnodar: KVVU, 2022. C.70-76
8. Zheng, Y. Dynamic defenses in cyber security: Techniques, methods and challenges / Y. Zheng, Z. Li, X. Xu // Digital Communications and Networks. — 2022. — № 8. — S. 422–435.
9. Shaping Attacker Behavior: Evaluation of an Enhanced Cyber Maneuver Framework / J. A. McKneely, T. K. Sell, K. A. Straub [i dr.] // HCII 2022: HCI for Cybersecurity, Privacy and Trust. — Cham: Springer, 2022. — S. 358–379. – DOI: 10.1007/978-3-031-05563-8_23
10. Lilli, E. How Can We Know What We Think We Know about Cyber Operations? / E. Lilli // Journal of Global Security Studies. — 2023. — № 8(2). — S. 1–18. – DOI 10.1093/jogss/ogad011
11. Dynamic-chaos information technologies for data transmission, storage, and protection / Yu. V. Gulyaev, R. V. Belyaev, G. M. Vorontsov [et al.] // Radioe`lektronika. Nanosistemy`. Informacionny`e texnologii. – 2018. – Vol. 10, No. 2. – P. 279-312. – DOI 10.17725/rensit.2018.10.279.
12. Chetvertakova, Yu. S. Postroenie modelej stoxasticheskix nelinejny`x dinamicheskix sistem na osnove dvuxe`tapnoj procedury` parametricheskoj identifikacii / Yu. S. Chetvertakova, O. S. Chernikova // Nauka. Texnologii. Innovacii: Sbornik nauchny`x trudov. V 9-ti chastyax, Novosibirsk, 30 noyabrya – 04 2020 goda / Pod redakciej A.V. Gadyukinoj. Tom Chast` 2. – Novosibirsk: Novosibirskij gosudarstvenny`j texnicheskij universitet, 2020. – S. 94-98.
13. Karganov, V. V. K voprosu o neobxodimosti modelirovaniya informacionny`x sistem organizacii, funkcioniruyushhix v usloviyax ugroz bezopasnosti / V. V. Karganov // Nacional`naya bezopasnost` Rossii: aktual`ny`e aspekty` : Sbornik statej Vserossijskoj nauchno-prakticheskoj konferencii, Sankt-Peterburg, 30 iyulya 2019 goda. – Sankt-Peterburg: Chastnoe nauchno-obrazovatel`noe uchrezhdenie dopolnitel`nogo professional`nogo obrazovaniya Gumanitarny`j nacional`ny`j issledovatel`skij institut «NACzRAZVITIE», 2019. – S. 20-30.
14. Budko, N. P. Obshhie principy` funkcionirovaniya i trebovaniya k postroeniyu struktur perspektivny`x sistem monitoringa raspredelenny`x informacionno-telekommunikacionny`x setej / N. P. Budko // Texnika sredstv svyazi. – 2021. – № 2(154). – S. 38-59.
15. Golovanov, A. A. Sravnitel`ny`j analiz sistem obnaruzhenij anomalij c ispol`zovaniem potoka setevogo trafika i protokola NETFLOW / A. A. Golovanov, O. I. Mel`nikova // Mezhdunarodny`j nauchno-issledovatel`skij zhurnal. – 2023. – № 6(132). – DOI 10.23670/IRJ.2023.132.18.
16. Poltavceva, M. A. Formirovanie struktur danny`x v zadachax aktivnogo monitoringa bezopasnosti // Problemy` informacionnoj bezopasnosti. Komp`yuterny`e sistemy`. – 2021. – № 1. – S. 9-19.
17. Alothman, B., Raw Network Traffic Data Preprocessing and Preparation for Automatic Analysis // 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). – 2019. – P. 1-5, DOI: 10.1109/CyberSecPODS.2019.8885333.
18. Chernigovskij, A. V. Ocenka stepeni samopodobiya setevogo trafika / A. V. Chernigovskij, M. V. Krivov // Informacionny`e texnologii. Problemy` i resheniya. – 2019. – № 1(6). – S. 115-120.
19. Chen, L. A deep multi-task representation learning method for time series classification and retrieval / L. Chen, D. Chen, F. Yang, J. Sun // Information Sciences. – 2021. – Vol. 555. – P. 17-32. – DOI 10.1016/j.ins.2020.12.062.
20. Kalinin, M. Yu. E`ntropijny`e ocenki reshayushhix statistik algoritma klassifikacii sluchajny`x processov / M. Yu. Kalinin, O. N. Choporov // Modelirovanie, optimizaciya i informacionny`e texnologii. – 2020. – T. 8, № 4(31). – DOI: 10.26102/2310-6018/2020.31.4.034.
21. Sokolovskij, S. P. Metodika formirovaniya lozhnogo setevogo trafika informacionny`x sistem dlya zashhity` ot setevoj razvedki / S. P. Sokolovskij, A. P. Telen`ga // Vestnik komp`yuterny`x i informacionny`x texnologij. – 2022. – T. 19, № 2(212). – S. 40-47. – DOI: 10.14489/vkit.2022.02.pp.040-047.