УДК 004.77; 004.94; 510.635.3

В.А. Овчаров

МОДЕЛИРОВАНИЕ СУБЪЕКТНО-ОБЪЕКТНОГО ВЗАИМОДЕЙСТВИЯ В СЕТЕВЫХ ИНФРАСТРУКТУРАХ

Овчаров В.А. **Моделирование субъектно-объектного взаимодействия в сетевых инфраструктурах.**
Аннотация. В работе рассматривается задача идентификации различных аспектов функционирования взаимодействующих объектов информационно-телекоммуникационных сетей (ИТКС) по результатам мониторинга сетевого трафика. В качестве решения данной задачи в части идентификации типов сетевых объектов и операций взаимодействия предлагается графовая модель поведения, в части деанонимизации отношений взаимодействующих объектов предложены предикатные модели состояний объектов информационно-телекоммуникационной сети (ИТКС) на основе отношений между экземплярами.
Ключевые слова: средства активной идентификации, средства пассивной идентификации, мониторинг сетевого трафика, сетевой процесс, контроль поведения, сетевой объект, информационно-телекоммуникационная сеть.

Ovcharov V.A. **Simulation of Subject-Object Interaction in Network Infrastructures.**
Abstract. The problem of identification of the different aspects of the interacting objects information and telecommunication networks (ITN) on the results of network traffic monitoring is analyzed. As a solution to this problem in terms of identifying the types of network facilities and operations interaction graph model of behavior is proposed, in terms of relations disclosure of anonymity interacting objects predicate state model objects ITN based on the relationship between instances is offered.
Keywords: active means of identification means of passive identification, network traffic monitoring, network process, behavior control, network object information and telecommunications network.

1. Введение. Современные ИТКС представляют собой сложные организационно-технические системы, состоящие из большого числа компонентов различной степени автономности, в разноплановой программно-аппаратной конфигурации, связанных между собой различными по используемым технологиям и скорости передачи данных каналами связи, обменивающиеся данными различных типов. Обеспечение сетевой безопасности и эффективного расследования компьютерных инцидентов, ставших реалиями современных ИТКС различного назначения, немыслимо без использования специалистами по сетевой криминалистике различных систем мониторинга, автоматизирующих процессы первичной обработки сетевого трафика и последующего анализа разнородной технической информации из различных источников.

Одной из наиболее актуальных задач перспективных систем мониторинга и обеспечения комплексной защиты информации в ИТКС является контроль действий приложений на сетевых узлах, сопостав-

ление идентифицированных процессов их взаимодействия с реальными пользователями и построение причинно-следственных связей для прогнозирования дальнейших действий пользователей.

В то же время разрабатываемые системы должны быть универсальными, обеспечивая работу как с различными источниками данных, так и в представленных на рисунке 1 сценариях (1 – сценарий сбора трафика на зеркалируемом интерфейсе, 2 – сценарий мониторинга количества и программно-аппаратных характеристик устройств, находящихся за NAT-/PAT-устройствами и межсетевыми экранами, 3 – сценарий мониторинга интерфейсов беспроводных сетей передачи данных и локальных беспроводных сегментов, 4 – сценарий мониторинга в качестве клиента проводного сегмента сети) использования в ИТКС различного типа. Данные сценарии обуславливают необходимость применения разрабатываемых моделей в ИТКС различного назначения и топологии, учета факторов большого количества узлов, программно-аппаратной неоднородности, динамики, существенной территориальной распределенности.

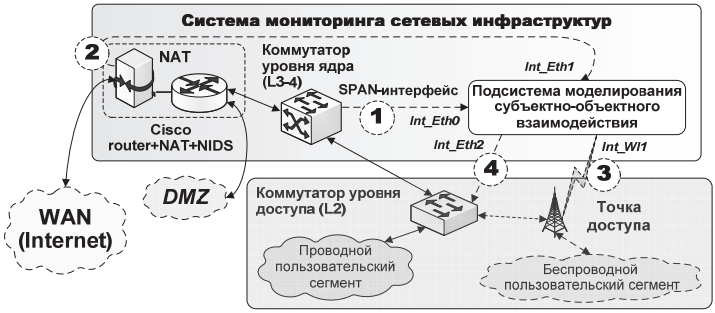

Рис. 1. Сценарии использования перспективных многофункциональных систем мониторинга ИТКС

Таким образом, при разработке соответствующих моделей (многомодельных комплексов) целесообразно употреблять термин «сетевая инфраструктура», подразумевая под ним возможность использования предлагаемых моделей в сетях различной архитектуры (одноранговой и клиент-серверной), типа (проводных IEEE 802.3 и беспроводных IEEE 802.11, 802.16), различных смешанных топологий [19]. В общем случае сетевая инфраструктура представляет собой граф:

$$G = (V, E),$$

где V – множество вершин (сетевых объектов), E – множество связей между сетевыми объектами.

Каждый сетевой объект V представляет собой структуру вида $\{x_1(t), x_2(t), \ldots, x_n(t)\}$, где $x_i(t)$ – параметр объекта, определенный в момент времени t и который может быть вычислен на основе обработки результатов мониторинга сетевого трафика. Таким образом, задача идентификации параметров сетевых объектов формулируется следующим образом: для каждого v из V определить вектор параметров v' и определить, насколько v' соответствует типовому профилю сетевого объекта из базы профилей.

Для решения данной задачи предлагается следующая функциональная декомпозиция. Концептуальная модель субъектно-объектного взаимодействия, учитывающая логические связи реальных пользователей ИТКС, ассоциированных носителей действий данных пользователей (набора идентификаторов, связанных с субъектом) и сетевыми объектами, идентифицируемыми средствами пассивного анализа сетевого трафика. Для выделения инициаторов информационного обмена разработана графовая модель поведения. Для формирования выводов по результатам анализа изменения состояний взаимодействующих экземпляров предложены предикатные модели пассивных и активных объектов ИТКС. В качестве подхода к решению проблемы наблюдаемости объектов ИТКС в информационном пространстве разработана модель ассоциированного представления процессов взаимодействия «субъект-различные типы устройств».

Специфика решаемой в работе задачи потребовала на первом этапе уточнения некоторых терминов и определений из работ [15, 16, 21], которые представлены следующим образом.

Мониторинг сетевого трафика – процесс систематического наблюдения за объектами и субъектами, влияющими на безопасность исследуемой ИТКС, сбора информации о параметрах состояния ее программно-аппаратных средств, социально-коммуникационных аспектах взаимодействия субъектов, сетевых и физических объектов, а также анализа и обобщения результатов наблюдений с целью фиксации соответствия (несоответствия) результатов первоначальным предположениям.

Сетевой процесс представляет собой профиль такого поведения ИТКС (динамической системы), которое заключается в исполнении действий по приему или передаче пакетов сетевого трафика или их преобразованию.

Коммуникационный протокол – совокупность правил, регламентирующих формат и процедуры обмена информацией между двумя или несколькими независимыми устройствами, компьютерами, программами или процессами.

Объект ИТКС – одна из сторон взаимодействия в ИТКС, ассоциированная с одним или несколькими субъектами, способная инициировать выполнение операций в соответствии с определенным протоколом.

Субъект ИТКС – ассоциированный с реальным пользователем носитель действий, поведение которого регламентируется политикой безопасности ИТКС или правилами разграничения доступа.

Пассивный мониторинг сетевых инфраструктур – комплекс технических мероприятий по сбору информации для формирования коммуникационных и поведенческих портретов объектов ИТКС на основе сбора, первичного анализа и декодирования сетевого трафика, а также информации уровня приложений на выбранном интерфейсе (группе интерфейсов), подмены и манипуляции данными без использования механизмов установления транспортных соединений.

Активный мониторинг сетевых инфраструктур – комплекс технических мероприятий по сбору информации для формирования коммуникационных и поведенческих портретов объектов ИТКС на основе анализа информации о состоянии коммуникационных портов, запущенных сервисах, службах, уязвимостях системного и прикладного ПО, доступности ресурсов, технологических процессах (циклах) функционирования, связанных с их работой, использующий механизмы установления транспортных соединений.

Коммуникационный портрет сетевых инфраструктур – форма описания и отображения характеристик сетевой инфраструктуры в целом и объекта ИТКС в части детализации правил (коммуникационных протоколов) и процедур обмена данными на соответствующем интервале наблюдения.

Поведенческий портрет сетевых инфраструктур – характерный индивидуальный штамп (параметрическое множество), характеризующий сферу профессиональных и личных интересов, кругозор, опыт, круг общения, образ и ритм жизни пользователей ИТКС.

2. Анализ существующих подходов к разработке моделей представления процессов функционирования сетевых инфраструктур. Вопросы сетевой анонимности в распределенных системах и идентификации злоумышленников на основе анализа трафика Tor-клиентов активно рассматриваются в работе [7]. Недостатком предложенных моделей и метрик является необходимость обеспечения доступа к магистральным каналам провайдеров уровня Tier-1, в то время как корректность работы предложенного симулятора TorPS и достоверность полученных результатов оценить невозможно из-за отсутствия доступа к приложению и его исходному коду.

Подавляющее большинство известных систем активного и пассивного мониторинга используют неформальные модели теории параметрической идентификации для выявления вредоносных http-запросов [13], а также сигнатурные методы [10], для которых на данный момент сложно получить теоретические оценки полноты, показать корректность, завершаемость [18, 4].

Средства пассивной идентификации (p0f, satori, network miner, caploader, Ettercap и др.) операционных систем (ОС) и компонент программного обеспечения (ПО) на основе анализа сетевого трафика и загружаемых дампов в различных форматах [19, 8, 12] используют модель вида

$$OSDef = \langle W, T, D, S, O, Q, OS, Det \rangle,$$

где W – значение поля WS (S_{nn} – кратный значению MSS, T_{nn} – кратный MTU), T – значение поля TTL, D – значение поля фрагментации, S – значение поля SYN, O – значение полей опций (N – NOP, E – EOL, W_{nnn} – значение опции масштабирования окна), M_{nnn} – максимальный размер сегмента, S – selective ACK OK, T – временная метка, T_0 – временная метка с нулевым значением), Q – опции (P – options past EOL, Z – значение поля IP ID, I – указанные параметры IP, U – URG-указатель, X – неиспользуемое ненулевое поле, A – число ACK, T – 2-я метка timestamp, F – различные нестандартные флаги (PUSH, URG и др.), D – данные полезной нагрузки, $!$ – опции (значения) некорректного сегмента, OS – тип ОС, Det – описание версии ОС.

В работе [17] разработаны технологии обнаружения и идентификации вредоносных программ на основе методов интеллектуального анализа данных. Выделены основные группы сущностей, используемых для формирования типовых методик обнаружения вредоносных программ на основе данной группы методов. Приведен обзор существующих методик обнаружения вредоносных программ на основе выделенных групп признаков, наборов данных, методов выделения значимых признаков и обучения, а также программных средств поддержки вычислений. Ограничением данных технологий является необходимость привлечения экспертов для разработки адекватных моделей процессов обучения и функционирования таких систем.

Средства активной идентификации ОС и ПО, сканеры портов и уязвимостей типа nmap, nessus, maxpatrol, используют модель вида [1]

$$OSDef = \langle W, M, T, Ws, S, N, D, T, F_n, L, OS \rangle,$$

где W – значение поля размера окна TCP Window Size, M – значение поля размера сегмента TCP Maximum Segment Size, T – значение поля

времени жизни TTL, *Ws* – значение опции масштабирования Window Scale, *D* – значение поля фрагментации, *S* – индикатор опции TCP SACK, *N* – индикатор опции TCP NOP, *D* – индикатор флага IP Don't Fragment, *T* – индикатор временной метки TCP Timestamp, F_n – индикатор флага пакета ($F_S = SYN$, $F_A = SYN+ACK$), *L* – значение длины пакета, *OS* – тип ОС.

Подход к построению систем анализа защищенности на основе активных методов, предложенный в работе [9] базируется на механизме автоматического генерирования и выполнения распределенных сценариев атак с учетом разнообразия целей и уровня знаний злоумышленника. В основе рассматриваемого подхода – комплексное использование основанных на экспертных знаниях моделей злоумышленника, вероятностных моделей ИТКС, генерации комплекса сценариев атак и оценки уровня защищенности.

В работе [1] был предложен, а в [6] – практически апробирован подход к идентификации компонент ПО на основе динамического сопоставления наблюдаемого поведения ОС или приложения с моделью его нормального поведения в виде альтернирующего автомата. В работах [12, 18] рассматриваются вопросы автоматического поиска уязвимостей и верификации протоколов и приложений с использованием эмпирических критериев допустимого поведения системы. Разработанные модели полны с точки зрения описания возможных отказов системы. В то же время, сложность [12] и узкая специализация сценариев использования предложенных в [11] решений позволяет эффективно использовать их на практике только в задачах аудита безопасности или отложенного расследования инцидентов.

Проведенный анализ [2, 3, 4, 14, 20] показал, что методы теории взаимодействующих последовательных процессов позволяют анализировать с приемлемой сложностью модели с очень большим и даже бесконечным множеством состояний. Применение научно-методического аппарата данной теории к задачам анализа сетевого трафика и расследования компьютерных инцидентов (сетевой криминалистики) возможно, в частности, благодаря разработанной в теории процессов технике символьных преобразований выражений, описывающих процессы.

Разработанные и описанные в данной работе модели проектировались как модели предметной области: сбор информации об объектах мониторинга целевой ИТКС средствами пассивной идентификации, для последующего обоснования корректности и оценки вычислительной сложности методов анализа разнородной технической информации из различных источников.

3. Концептуальная модель субъектно-объектного взаимодействия в ИТКС. Представим исследуемую ИТКС как множество взаимодействующих экземпляров типов объектов. Будем выделять 2 типа объектов ИТКС: программные и аппаратные.

Программные объекты ИТКС разделим на *одноузловые* (экземпляры ОС, ПО на узлах ИТКС, взаимодействующие в рамках одного узла (локально)) и *многоузловые* (экземпляры ПО на узлах ИТКС и внешних ресурсах, взаимодействующие с различными узлами ИТКС).

Аппаратные объекты ИТКС включают в себя активное сетевое оборудование (коммутаторы, маршрутизаторы, точки доступа, шлюзы, межсетевые экраны (МСЭ)), серверное оборудование, различные датчики и сенсоры систем обнаружения атак и мониторинга (DPI), пассивное сетевое оборудование (каналообразующая аппаратура) и радиомодемы, локальные ПЭВМ, физические каналы связи между узлами ИТКС (ПЭВМ), мобильные персональные устройства (МПУ).

Множество программных и аппаратных объектов некоторой ИТКС могут взаимодействовать друг с другом (внутри ИТКС), с аналогичными объектами других ИТКС (например, используя инфраструктуру VPN), или внешними объектами (например, web- или DNS-серверами глобальных сетей). С каждым объектом ИТКС может быть однозначно ассоциирован некоторый субъект, структура которого будет подробно рассмотрена в п.6. В общем случае субъекты могут быть ассоциированы (быть наблюдаемы) как с объектами целевой ИТКС (объекта мониторинга), так и с объектами (как внутренними, так и внешними) других ИТКС в соответствии с особенностями информационного обмена объектов целевой ИТКС.

Концептуальная модель субъектно-объектного взаимодействия в ИТКС представлена на рисунке 2. В разработанной модели приняты следующие обозначения: $T^{(1)}$ – цель мониторинга (подсеть, отдельный сегмент ИТКС, распределенная ИТКС, web-ресурс и пр.), $\{U_{Ti}\}$ – множество реальных (физических) пользователей, ассоциированных с целью мониторинга, $\{Obj^{(1)}\}$ – множество объектов цели (ИТКС), идентифицированных системой мониторинга, $T^{(2)}$ – сегмент ИТКС аналогичного объекта (внутренняя подсеть или ресурс), $T^{(3)}$ – внешний ресурс в глобальной сети или территориально-распределенная (многосегментная, многофилиальная) ИТКС, $Res_{loc_1}^{(1)}$ – внутренние ресурсы цели мониторинга, Res^{ext} – внешние ресурсы, связанные в объектами ИТКС (цели мониторинга), $Obj^{1)}$ – наблюдаемые объекты ИТКС $T^{(1)}$, взаимодействующие в рамках политики безопасности и коммуникаци-

онных протоколов, $Subj^{(1)}$ – идентифицированные в процессе мониторинга субъекты ИТКС $T^{(1)}$.

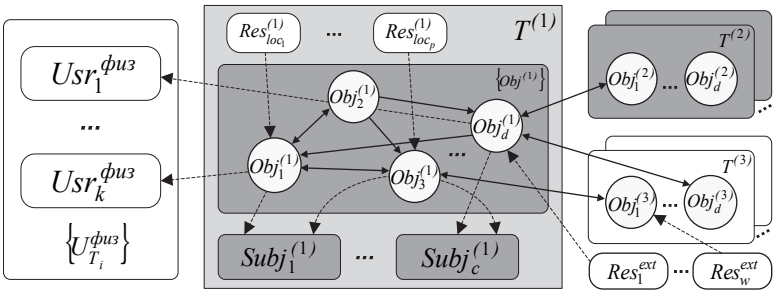

Рис. 2. Концептуальная модель субъектно-объектного взаимодействия в ИТКС

Интерпретация субъекта в соответствии с п.3 связана с тем, что реальный пользователь не имеет доступа к сетевым объектам напрямую, а осуществляет его, используя различные идентификаторы, учетные записи и соответствующие процедуры аутентификации и авторизации. Именно субъекты ИТКС в результате анализа и обобщения результатов мониторинга должны быть корректно сопоставлены с реальными пользователями ИТКС.

4. Графовая модель поведения объектов мониторинга. Разделим множество объектов ИТКС на два подмножества: подмножество активных и подмножество пассивных объектов. Пассивный объект ИТКС не может в данный момент времени осуществлять доступ (инициировать TCP-/UDP-взаимодействие) к другим объектам, в то время как активный – может.

Введем следующие обозначения: A – множество типов активных объектов ИТКС, R_c – множество экземпляров активных объектов ИТКС, P – множество типов пассивных объектов ИТКС, R_p – множество экземпляров пассивных объектов ИТКС, тогда

$$R = R_c \cup R_p .$$

Полагаем $R_c \cap R_p = 0$.

Для каждого типа объекта ИТКС $r_i \in R$ определены соответствующие операции доступа с использованием определенного типа протокола и номера TCP-/UDP-порта (прием/отправка e-mail, обновление ОС и прикладного ПО, чтение/запись на удаленном сервере, использование web-браузера, файловый обмен, запуск на исполнение и т.д.). При этом, доступ к соответствующему объекту ИТКС может быть как

непосредственным, так и косвенным – через другие объекты. Доступ по некоторой операции к объекту ИТКС подразумевает выполнение последовательности элементарных операций в соответствии с логикой работы используемого протокола. Предполагаем, что в ходе реализации доступа объектов в исследуемой ИТКС элементарные операции в рамках коммуникационных протоколов выполняются мгновенно, но, в ряде случаев, могут отстоять друг от друга во времени. Данная ситуация обусловлена временными интервалами мониторинга, в которых возможно несколько элементарных операций, ассоциированных с одним объектом ИТКС (параллельное или последовательное обращение к одному или нескольким объектам).

Пусть r – экземпляр объекта ИТКС типа *type*, представляемый пятеркой вида

$$r = \langle ID, type, \xi, O, T, \rho, \iota \rangle,$$

где *ID* – идентификатор (имя экземпляра) объекта ИТКС, *type* – тип объекта, где $type \in A \cup P$, ξ – значение показателя скомпрометированности экземпляра объекта ИТКС, O – множество операций взаимодействия, определенных (идентифицируемых системой мониторинга) для данного типа объектов, T – значение порога компрометации объектов ИТКС данного типа, ρ – значение показателя доступности объекта ИТКС, ι – индикатор протокола взаимодействия, причем

$$O = \{o_1, o_2, o_3, o_4, o_5, o_6, o_7, o_8, o_9\},$$

где o_1 – использование служб фоновой передачи (BITS) для обновления, o_2 – аутентификация, o_3 – запрос характеристик ПЭВМ объектом назначения, o_4 – VPN-соединение, o_5 – SSL-соединение, o_6 – VoIP-взаимодействие, o_7 – DNS-взаимодействие с использованием DNSSEC, o_8 – RDP-взаимодействие, o_9 – TOR-взаимодействие.

Представленная пятерка формирует поведенческий портрет каждого экземпляра объекта ИТКС. Графовая модель поведения объектов мониторинга на множестве экземпляров объектов ИТКС в некотором ее состоянии представлена на рисунке 3.

Определим ξ и T как переменные на R со значениями в [0, 1], ι – как переменную со значениями [0, 255], соответствующими коммуникационному протоколу, с использованием которого осуществляется взаимодействие между объектами ИТКС, а ρ – как переменную со значениями [0, 65535], соответствующими количеству портов TCP/UDP, с использованием которых осуществляется взаимодействие

между объектами ИТКС. Будем понимать под значением $\xi(r)$ текущее состояние (не скомпрометирован, скомпрометирован) объекта $r \in R$. Считаем, что если $\xi(r) > T(r)$, то поведение объекта $r \in R$ не определено, а его состояние опасное (в случае мониторинга защищаемой ИТКС), или атакуемое (в случае мониторинга целевой ИТКС).

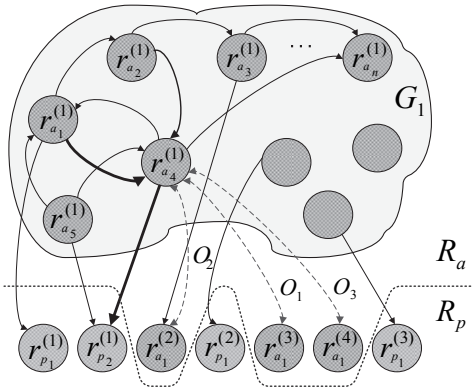

Рис. 3. Графовая модель поведения объектов мониторинга в некотором состоянии ИТКС

Следует отметить, что подсистема визуализации разработанных моделей должна разрешать основное противоречие познания – между *сукцессивностью* (некоторой последовательностью) представления результатов мониторинга и *симультанностью* (одновременностью) их понимания и интерпретации аналитиком. Отсутствие подходов к его разрешению в существующих программно-аппаратных комплексах мониторинга делает их использование неэффективным в повседневной работе аналитика при решении нетривиальных задач и принятии решений. В этой связи необходимо разработать такую подсистему, целевое использование которой позволит оперативно идентифицировать определенные аспекты взаимодействия объектов мониторинга исключительно на основе технологий пассивного анализа сетевого трафика, используя предложенные выше модели. Так, представленная ниже графовая модель (карта ИТКС) позволяет уже на первом этапе разложения графа на плоскости в соответствии с используемым алгоритмом выделить основных инициаторов информационного обмена и их географическое местоположение.

Исходя из приведенных соображений и обозначенных в п.1 сценариев применения систем мониторинга при разработке подсистемы визуализации результатов анализа взаимодействия объектов ИТКС

использовались визуальные средства на основе следующих критериев: разработаны на языке C++, открытый исходный код, мультиплатформенность, лицензия GPLv3. Функциональное представление компонента визуализации (плагина) – кнопка на панели инструментов, при нажатии на которую графовая модель (граф) в соответствующем диалоге изменяется по следующим параметрам: уменьшается число пересечений дуг, среднее расстояние между узлами, дуги могут быть представлены ортогонально, в виде прямых линий. На рисунке 4 приведен пример разложения графа на плоскости (построения карты сети по результатам анализа взаимодействия объектов ИТКС) с использованием разработанного компонента визуализации (библиотеки).

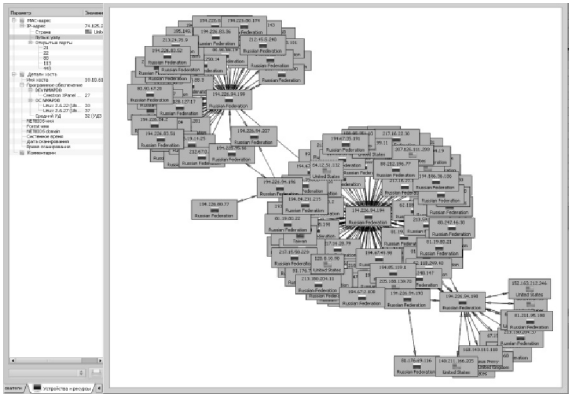

Рис. 4. Пример разложения графа на плоскости (построение карты сети по результатам анализа взаимодействия объектов ИТКС) с использованием разработанного компонента визуализации

Библиотека включает базовые структуры данных, различные классы графов и алгоритмов разложения, которые можно настраивать и изменять с использованием встроенных модулей. В базовые структуры данных, кроме массивов, строк, очередей входят элементы для параллельного программирования (мьютекс, барьер, критическая секция, поток).

5. Предикатные модели состояний объектов ИТКС на основе отношений между экземплярами. Пусть для каждой пары экземпляров объектов ИТКС (r_i, r_j), где $r_i \in R_c, r_j \in R$ системой мониторинга идентифицирована операция взаимодействия $a \in A_{r_j}$, связанная с обращением объекта r_i к r_j с использованием соответствующего про-

токола и порта, тогда предикатная модель (предикат), определяющая отношение взаимодействующих объектов будет иметь вид:

$$a(r_i,r_j)\equiv 1 \Leftrightarrow a\in A_{r_j}\, u(a,r_i,r_j)\in \psi(r_i,r_j),$$

где $\psi(r_i,r_j)=\left\{(a,r_i,r_j)\mid a\in A_{r_j}, r_i\in R_c, r_j\in R\right\}$ – отношение инициализации сессии при взаимодействии объектов r_i и r_j.

Замечание: отношение взаимодействующих объектов не симметрично по $r\in R$ и не транзитивно.

Обозначим тройку $(a,r_i,r_j)\in\psi(r_i,r_j)$ как $\psi_a(r_i,r_j)$, так как это отношение на $R_c\times R$.

В реальных ИТКС пользователи часто используют средства анонимизации типа TOR для разрыва причинно-следственных связей и затруднения работы систем мониторинга. В таких ситуациях взаимодействие объектов может быть не только непосредственным, но и транзитивным, когда один или несколько объектов используют несколько других объектов через цепочку операций взаимодействия. Другим примером является ситуация, когда удаленный пользователь при обращении к терминальному ssh-серверу запускает на выполнение экземпляр сервера, который, в свою очередь, запускает на выполнение определенную программную оболочку или среду виртуальных машин (ВМ), которая, также по командам от пользователя, инициирует новые процессы. При этом все процессы и экземпляры ВМ будут трактоваться как пассивные объекты ИТКС. Последовательность объектов от клиента до конечного пассивного объекта ИТКС при выполнении соответствующей операции будет транзитивным замыканием операции.

Определим подмножество множества активных объектов ИТКС, для которых отношение инициализации сессии по какой-либо операции транзитивно:

$$R_c^{G_1}=\left\{\begin{matrix} r_{a_4}^{(1)}\in R\ \exists a:\forall r_{a_1}^{(1)},r_{p_2}^{(1)}\in R: r_{a_1}^{(1)}\to r_{a_4}^{(1)}, r_{a_4}^{(1)}\to r_{p_2}^{(1)},\\ r_{a_4}^{(1)}\in R\ \exists a:\forall r_{a_2}^{(1)},r_{p_2}^{(1)}\in R: r_{a_2}^{(1)}\to r_{a_4}^{(1)}, r_{a_4}^{(1)}\to r_{p_2}^{(1)},\end{matrix}\right\}$$

Представим состояние экземпляра пассивного объекта ИТКС r_p тройкой вида:

$$S_{r_p}=(In(r),I(\xi(r_p)),\rho(r_p),\iota(r_p),\vartheta(r_p),\theta(r_p)),$$

где $In(r)=\left\{r\in R_c\mid \exists a\in A_{r_p}: r\to r_p\right\}$ – множество экземпляров объектов, инициирующих и осуществляющих взаимодействие с r_p, $I(\xi(r_p))=[0,1]$ –

индикатор скомпрометированности экземпляра пассивного объекта ИТКС, $\rho(r_p) = [0,65535]$ – индикатор TCP/UDP-взаимодействия (порта) экземпляра пассивного объекта ИТКС, $\iota(r_p) = [0,255]$ – индикатор протокола взаимодействия (на основе значений поля IPProto) экземпляра пассивного объекта ИТКС, $\vartheta(r_p) = [0,281\ 474\ 976\ 710\ 655]$ – адресный индикатор, $\theta(r_p)$ – DNS-индикатор (доменный индикатор).

Аналогично представим состояние экземпляра активного объекта ИТКС r_c:

$$S_{r_c} = (In(r_c), From(r_c), I(\xi(r_c)), \rho(r_c), \iota(r_c), \vartheta(r_c), \theta(r_c)),$$

где $In(r_c) = \{r \in R_c \mid \exists a \in A_{r_c} : r \to r_c\}$ – множество экземпляров активных объектов ИТКС, инициирующих и осуществляющих непосредственное взаимодействие с r_c, $From(r_c) = \{r \in R \mid \exists a \in A_{r_c} : r_c \to r\}$ – множество экземпляров объектов ИТКС, к которым r_c осуществляет непосредственный доступ и взаимодействие, $I(\xi(r_c)) = [0,1]$ – индикатор скомпрометированности экземпляра активного объекта ИТКС, $\rho(r_c) = [0,65535]$ – индикатор TCP/UDP-взаимодействия (порта) экземпляра активного объекта ИТКС, $\iota(r_c) = [0,255]$ – индикатор протокола взаимодействия (на основе значений поля IPProto) экземпляра активного объекта ИТКС, $\vartheta(r_c) = [0,281\ 474\ 976\ 710\ 655]$ – адресный индикатор, $\theta(r_c)$ – DNS-индикатор (доменный индикатор).

Представленные выражения для состояний экземпляров активных и пассивных объектов ИТКС позволяют сделать вывод о том, что при инициализации соединения и осуществлении дальнейшего взаимодействия некоторого экземпляра объекта ИТКС с соответствующим экземпляром другого объекта изменяются состояния обоих взаимодействующих экземпляров. Таким образом, основной функцией подсистемы анализа аспектов субъектно-объектного взаимодействия является построение дискретно-временной шкалы взаимодействия экземпляров объектов и динамически обновляемой объектной модели данных, отражающей специфику их связей в виде множества узлов и ребер. Узлы и ребра имеют конечный набор атрибутов-идентификаторов: индикатор порта p, протокола l, DNS-имени θ, IP-адреса ϑ. Вся последующая этапу первичной обработки работа системы мониторинга осуществляется с синтезированными или динамически обновленными по результатам первичной обработки предикатными моделями.

6. Модели ассоциированного представления субъектно-объектного взаимодействия. Проблема наблюдаемости объектов ИТКС в информационном пространстве имеет двоякий характер. С одной стороны, она обусловлена тем, что в настоящее время практически каждый реальный пользователь ИТКС использует в различных сетях различные типы устройств: в локальном сегменте ИТКС организации – инфраструктуру терминальных серверов и «тонких клиентов», стационарные ПЭВМ, серверы (рабочие станции) или мобильные рабочие места (МРМ) типа ноутбук, дома, как правило, МРМ, ПЭВМ или мобильной персональное устройство (МПУ), в общественных местах и при перемещениях – МПУ или МРМ. Таким образом, с реальным пользователем (человеком) должны быть корректно ассоциированы все используемые им устройства (типы устройств). Модель ассоциированного представления взаимодействия «субъект-типы устройств» (рисунок 5), призвана решить данный аспект проблемы наблюдаемости объектов ИТКС.

В приведенной модели приняты следующие обозначения: ID^A – персональный идентификатор, ID^B – идентификатор должности в организации (должностной идентификатор), ID^C – идентификатор номера рабочего телефона/факса, ID^D – аппаратный идентификатор (MAC-адрес, IMEI, IMSI, IMN, FHIN, RHIN), ID^F – логический идентификатор (ID VK, e-mail, номер телефона, login), ID^G – идентификатор социальной (тематической) группы, ID^H – AD-идентификатор, $NIC_1, ..., NIC_J$ – сетевое имя-псевдоним персоны.

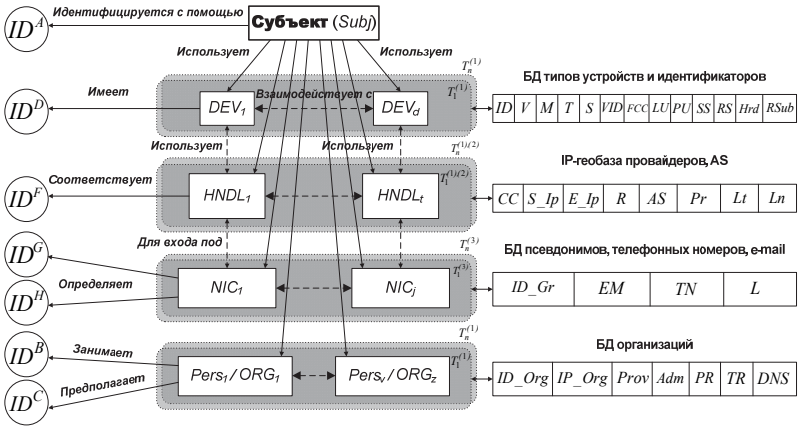

Рис. 5. Схема модели ассоциированного представления процессов взаимодействия «субъект-различные типы устройств»

Столбцы таблиц базы данных (БД) имеют следующие обозначения: *V* – производитель, *M* – модель, *T* – тип, *S* – стандарт, *VID* – идентификатор производителя, *FCC* – FCC-идентификатор, *LU* – login пользователя, *PU* – пароль пользователя, *SS* – тип и версия ПО, *RS* – используемые технологии шифрования, *Hrd* – другие особенности аппаратной части, *Rsub* – особенности радиоподсистемы, *CC* – код страны, *S_Ip* – начальный IP-адрес диапазона, *E_Ip* – конечный IP-адрес диапазона, *R* – идентификатор региона, *AS* – номер автономной системы, *Pr* – наименование провайдера, *Lt* – широта, *Ln* – долгота, *ID_Gr* – идентификатор группы, *EM* – адрес электронной почты, *TN* – номер телефона, *L* – login, *ID_Org* – идентификатор организации, *IP_Org* – IP-адреса организации, *Prov* – реквизиты провайдера, *Adm* – реквизиты администраторов (группы технической поддержки), *PR* – значение page rank, *TR* – значение traffic rank, *DNS* – DNS-имя.

С другой стороны, в реальных ситуациях взаимодействующие объекты мониторинга могут находиться как одном или в различных сегментах целевой ИТКС, так и в различных, территориально распределенных ИТКС. Для решения данного аспекта проблемы наблюдаемости объектов ИТКС разработана модель представления процессов мониторинга, обработки и хранения результатов обработки, формализуемая четверкой вида:

$$M_i: \left\langle S_k, D_l^{dest}, C_m^{dest}, I_p \right\rangle,$$

где S_k – источник информации (объект мониторинга), $k \in N_k$; D_l^{dest} – получатели информации (средства мониторинга (наблюдения)), $d \in N_d$; C_m^{dest} – средства хранения информации, $c \in N_c$; I_p – информационные каналы (каналообразующие средства).

На основе анализа решаемых задач, архитектуры, особенностей программной реализации и специфики взаимодействия функциональных подсистем современных систем мониторинга ИТКС предложена таксономическая схема процессов сбора, обработки и хранения данных мониторинга (рисунок 6), позволяющая синтезировать структурные логико-графические модели систем мониторинга ИТКС различной архитектуры и назначения.

Автоматизация построения подобных моделей представляет собой трудно формализуемую задачу, решаемую, как правило, исследователем эвристически на основе последовательного анализа структуры системы «сверху–вниз». Построение адекватных реальным системам моделей возможно только на основе глубокого знания структуры системы и отдельных подсистем, особенностей функционирования, спе-

цифики информационных потоков и условий эксплуатации. Кроме того, необходимо совершенно чётко представлять возможности обеспечивающих подсистем (резервирования, восстановления и др.) применительно к каждому элементу системы.

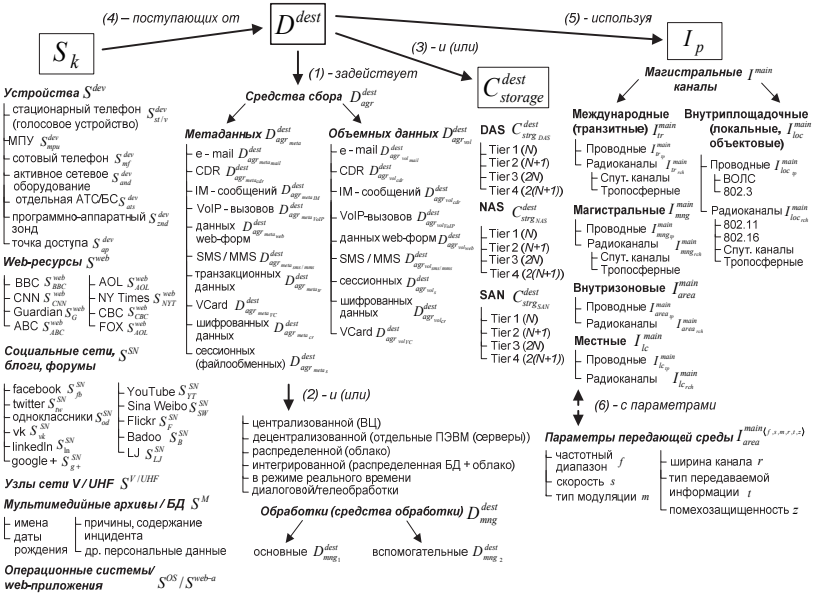

Рис. 6. Таксономическая схема процессов сбора, обработки и хранения данных мониторинга

В соответствии с введенной таксономической схемой типовая модель процессов взаимодействия компонент распределенной системы мониторинга ИТКС (коммуникационный портрет) имеет вид:

$$M : \left\langle \begin{Bmatrix} s^{dev}_{st/v} \cup s^{dev}_{mpu} \cup s^{dev}_{ats} \cup s^{dev}_{mf} \cup s^{dev}_{znd} \end{Bmatrix} \begin{Bmatrix} d^{dest}_{agr_{meta}} \cup d^{dest}_{agr_{volVoIP}} \cup d^{dest}_{mng_2} \end{Bmatrix} \begin{Bmatrix} c^{dest}_{storage_{DAS}} \cup c^{dest}_{storage_{NAS}} \end{Bmatrix} \begin{Bmatrix} i^{main}_{lc} \cup i^{main}_{mng} \cup i^{main}_{area} \end{Bmatrix} \right\rangle .$$

7. Заключение. Таким образом, практическое использование разработанных моделей для систем мониторинга ИТКС позволяет эффективно комбинировать или агрегировать в одном программно-аппаратном комплексе (ПАК) технологии активного, пассивного и квазипассивного сбора информации, использовать различные БД при обработке результатов мониторинга. Описанные модели легли в осно-

ву модуля квазипассивного мониторинга, входящего в состав распределенной аналитической системы. В сравнении с известными сканерами портов и уязвимостей (acunetics, nmap, zmap, OpenVAS, MaxPatrol, wikto и др.) существенно снижена продолжительность сеанса мониторинга. Отличительной особенностью реализации и комбинированного использования технологий пассивного и квазипассивного мониторинга является использование геобаз на различных этапах (как первичной, так и вторичной) обработки результатов мониторинга, whois-сервисов, централизованное хранение параметров сетевых объектов и типовых профилей в распределенной БД, загрузка/выгрузка дампов мониторинга и результатов обработки в различных форматах.

Все модули ПАК имеют открытый исходный код. В перспективе данный проект планируется развивать в следующих направлениях:

– разработки децентрализованной подсистемы накопления данных об объектах ИТКС;

– разработки метода учета динамики изменения свойств объектов ИТКС;

– разработки технологий многомерного отображения объектов и субъектов ИТКС;

– совершенствования методик анализа сетевого трафика.

Литература

1. *Allen J.M.* OS and Application Fingerprinting Techniques. SANS Institute. 2008.
2. *Arcolano N., Miller B.A.* Statistical Models and Methods for Anomaly Detection in Large Graphs // SIAM Annual Meeting. Minisymposium «Massive Graphs: Big Compute Meets Big Data». 2012.
3. *Beard M.S., Bliss N.T., Miller B.A.* Matched Filtering for Subgraph Detection in Dynamic Networks // Proceedings of the IEEE Statistical Signal Processing Workshop. 2011. pp. 509–512.
4. *Chitpranee R., Fukuda K.* Towards passive DNS software fingerprinting // AINTEC'13 Proceedings of the 9th Asian Internet Engineering Conference. 2013. pp. 9–16.
5. *Gordon L.* Nmap reference guide. URL: http://nmap.org/.
6. P0f v3 (version 3.08b). URL: http://lcamtuf.coredump.cx/p0f3/
7. *Johnson A., Wacek C.* Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries // 20th ACM Conference on Computer and Communications Security. 2013. pp. 337–348.
8. *Kollmann E.* Satori homepage. URL: http://myweb.cableone.net/xnih/.
9. *Kotenko I., Stepashkin M.* Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle // Lecture Notes in Computer Science. The Third International Workshop «Mathematical Methods, Models and Architectures for Computer Networks Security» (MMM-ACNS-05). Springer-Verlag. vol. 3685. 2005. pp. 317–330.
10. *Matousek P., Rysavy O., Gregr M.* Towards Identification of Operating Systems from the Internet Traffic. IPFIX Monitoring with Fingerprinting and Clustering // Proceedings of the 5th International Conference on Data Communication Networking

(DCNET 2014). Wien: SciTePress – Science and Technology Publications. 2014. pp. 21–27.
11. *Nguyen L.T., Zhang J.* Wi-Fi fingerprinting through active learning using smartphones // Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication. 2013. pp. 969–976.
12. *Ornaghi A.* Ettercap. URL: http://ettercap.github.io/ettercap/.
13. Särökaari N. How to identify malicious HTTP Requests // SANS Institute. 2012. 25 p.
14. *Shaner R.A.* US Patent No. 5991714. 1999.
15. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения // М.: Госстандарт России. 2006.
16. *Дождиков В.Г.*, *Салтан М.И.* Краткий энциклопедический словарь по информационной безопасности // М.: "Энергия". 2012. 240 с.
17. *Комашинский Д.В., Котенко И.В.* Методы интеллектуального анализа данных для выявления вредоносных программных объектов: обзор современных исследований // Вопросы защиты информации. 2013. № 4. С. 21–33.
18. *Смелянский Р.Л.* Модель поведения сетевых объектов в распределённых вычислительных системах // Программирование. 2007. № 4. С. 20–31.
19. *Таненбаум Э., Уэзеролл Д.* Компьютерные сети. Пятое издание // Спб.: "Питер". 2012. 960 с.
20. *Хоар Ч.* Взаимодействующие последовательные процессы // М.: "Мир". 1989. 264 с.
21. *Черемушкин А.В.* Информационная безопасность. Глоссарий // М.: "АВАНГАРД ЦЕНТР". 2013. 322 с.

References

1. Allen J.M. OS and Application Fingerprinting Techniques. SANS Institute. 2008.
2. Arcolano N., Miller B.A. Statistical Models and Methods for Anomaly Detection in Large Graphs. SIAM Annual Meeting. Minisymposium «Massive Graphs: Big Compute Meets Big Data». 2012.
3. Beard M.S., Bliss N.T., Miller B.A. Matched Filtering for Subgraph Detection in Dynamic Networks. Proceedings of the IEEE Statistical Signal Processing Workshop. 2011. pp. 509–512.
4. Chitpranee R., Fukuda K. Towards passive DNS software fingerprinting. AINTEC'13 Proceedings of the 9th Asian Internet Engineering Conference. 2013. pp. 9–16.
5. Gordon L. Nmap reference guide. URL: http://nmap.org/.
6. P0f v3 (version 3.08b). URL: http://lcamtuf.coredump.cx/p0f3/
7. Johnson A., Wacek C. Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries. 20th ACM Conference on Computer and Communications Security. 2013. pp. 337–348.
8. Kollmann E. Satori homepage. URL: http://myweb.cableone.net/xnih/.
9. Kotenko I., Stepashkin M. Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle. Lecture Notes in Computer Science. The Third International Workshop «Mathematical Methods, Models and Architectures for Computer Networks Security» (MMM-ACNS-05). Springer-Verlag. vol. 3685. 2005. pp. 317–330.
10. Matousek P., Rysavy O., Gregr M. Towards Identification of Operating Systems from the Internet Traffic. IPFIX Monitoring with Fingerprinting and Clustering. Proceedings of the 5th International Conference on Data Communication Networking (DCNET 2014). Wien: SciTePress – Science and Technology Publications. 2014. pp. 21–27.

11. Nguyen L.T., Zhang J. Wi-Fi fingerprinting through active learning using smartphones. Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication. 2013. pp. 969–976.
12. Ornaghi A. Ettercap. URL: http://ettercap.github.io/ettercap/.
13. Särökaari N. How to identify malicious HTTP Requests. SANS Institute. 2012. 25 p.
14. Shaner R.A. US Patent No. 5991714. 1999.
15. GOST R 50922-2006. [Protection of information. Basic terms and definitions]. M.: Gosstandart Rossii. 2006. (In Russ.).
16. Dozhdikov V.G. *Kratkiy entsiklopedicheskiy slovar' po informatsionnoy bezopasnosti* [Short Encyclopedic Dictionary of Information Security]. M.: Energy. 2012. 240 p. (In Russ.).
17. Komashinskiy D.V., Kotenko I.V. [Data mining techniques to identify malicious software Ob-projects: a review of current research]. *Voprosy zashchity informatsii – Problems of information security*. 2013. vol. 4. pp. 21–33. (In Russ.).
18. Smelyanskiy R.L. [Behavioral model of network objects in distributed computing systems]. *Programmirovaniye – Programming*. 2007. vol. 4. pp. 20–31. (In Russ.).
19. Tanenbaum E., Uezeroll D. *Komp'yuternyye seti. Pyatoye izdaniye* [Computer networks. Fifth Edition]. Spb.: Piter. 2012. 960 p. (In Russ.).
20. Hoare C. *Vzaimodeystvuyushchiye posledovatel'nyye protsessy* [Communicating Sequential Processes]. M.: "The World". 1989. 264 p. (In Russ.).
21. Cheremushkin A.V. *Informatsionnaya bezopasnost'. Glossariy.* [Information security. Glossary]. M.: "AVANGUARD CENTER". 2013. 322 p. (In Russ.).

Овчаров Владимир Александрович — к-т техн. наук, докторант кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: технологии мониторинга сетей, анализ трафика, кластерный анализ, теория вычислительной сложности, расследование инцидентов информационной безопасности. Число научных публикаций — 36. 9823800@inbox.ru; ул. Ждановская, д 13, Санкт-Петербург, 197198; р.т.: +7(812)237-19-60.

Ovcharov Vladimir Aleksandrovich — Ph.D., doctoral student of systems for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: technology network monitoring, cluster analysis, network situational awareness, computational complexity, network forensics, traffic analysis. The number of publications — 36. 9823800@inbox.ru; 13, Zhdanovskay street, St.-Petersburg, 197198, Russia; office phone: +7(812)237-19-60.

РЕФЕРАТ

Овчаров В.А. **Моделирование субъектно-объектного взаимодействия в сетевых инфраструктурах.**

В работе рассматривается задача разработки моделей поведения объектов сетевых инфраструктур (пользователей, устройств и ресурсов) по результатам анализа субъектно-объектного взаимодействия. В качестве решения данной задачи в части идентификации типов сетевых объектов и операций взаимодействия предлагается графовая модель поведения, в части деанонимизации отношений взаимодействующих объектов предложены предикатные модели состояний объектов информационно-телекоммуникационной сети (ИТКС) на основе отношений между экземплярами.

На основе анализа решаемых задач, архитектуры, особенностей программной реализации и специфики взаимодействия функциональных подсистем современных систем мониторинга ИТКС предложена таксономия процессов сбора, обработки и хранения данных мониторинга, позволяющая синтезировать структурные логико-графические модели систем мониторинга ИТКС различной архитектуры и назначения.

SUMMARY

Ovcharov V.A. **Simulation of Subject-Object Interaction in Network Infrastructures.**

The problem of modeling the behavior of objects network infrastructures (users, devices, and resources) for the analysis of subject-object interaction is considered. As a solution to this problem in terms of identifying the types of network facilities and operations interaction graph model of behavior is proposed, in terms of relations disclosure of anonymity interacting objects predicate state model object information and telecommunications network (ITN) on the basis of relations between instances is offered.

Based on the analysis of tasks, architecture, features software implementation and specific interaction of functional subsystems of modern monitoring systems of ITN taxonomy of the collection, processing and storage of monitoring data, which allows to synthesize structural logic-graphic model of monitoring systems ITN different architecture and destination, is proposed.