УДК: 004.056 DOI: 10.53816/23061456_2022_7–8_94

ПРИНЦИПЫ СЕМИОТИЧЕСКОГО МОДЕЛИРОВАНИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В ПРИЛОЖЕНИИ К ЗАДАЧАМ ВНЕШНЕГО ПРОЕКТИРОВАНИЯ ПРОАКТИВНЫХ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ОЦЕНИВАНИЯ ЭФФЕКТИВНОСТИ ИХ ПРИМЕНЕНИЯ

PRINCIPLES OF SEMIOTIC MODELING OF INTRUSION DETECTION SYSTEMS IN APPLICATION TO THE TASKS OF EXTERNAL DESIGN OF PROACTIVE INFORMATION SECURITY SYSTEMS AND EVALUATION OF THE EFFECTIVENESS OF THEIR APPLICATION

Канд. техн. наук А.М. Сухов, д-р техн. наук А.В. Крупенин, канд. экон. наук М.П. Табункова

Ph.D. A.M. Sukhov, D.Sc. A.V. Krypenin, Ph.D. M.P. Tabunkova

Краснодарское высшее военное училище им. С.М. Штеменко

В статье рассматривается комплексный подход к исследованию качества функционирования целеустремленных технических систем в критической информационной инфраструктуре. Особенность предлагаемого подхода моделирования заключается в комплексном учете всех факторов, влияющих на эффективность исследуемого процесса. Раскрыты характеристики, позволяющие рассматривать объекты критической информационной инфраструктуры через призму сложных систем. Поставлена задача априорного оценивания эффективности деструктивного воздействия виртуального злоумышленника. Описаны принципы семиотического моделирования объектов критической информационной инфраструктуры при симбиозном взаимодействии с эвентуальным злоумышленником.

Ключевые слова: система обнаружения вторжений, эффективность целевого применения, вторжение, теория эффективности, проактивность, информационная безопасность, критическая информационная инфраструктура.

The article considers a comprehensive approach to the study of the quality of functioning of purposeful technical systems in critical information infrastructure. The peculiarity of the proposed modeling approach is the comprehensive consideration of all factors affecting the effectiveness of the process under study. The characteristics allowing to consider objects of critical information infrastructure through the prism of complex systems are disclosed. The tasks of a priori evaluation of the effectiveness of the destructive impact of a virtual attacker are set. The principles of semiotic modeling of critical information infrastructure objects in symbiotic interaction with an eventual attacker are described.

Keywords: intrusion detection system, target application efficiency, intrusion, efficiency theory, proactivity, information security, critical information infrastructure.

Введение

Особенностью противоборства конфликтующих целеустремленных технических систем в информационном конфликте являются одинаковые условия функционирования их средств воздействия и средств обнаружения этих воздействий. Под условиями функционирования следует понимать некоторую среду — «площадку», на которой происходит конфликт. В киберпространстве этой средой является критическая информационная инфраструктура (КИИ), характеристики которой (вектор $\mathbf{B}'_{\langle l'\rangle}$) оказывают влияние на параметры и эксплуатационно-технические характеристики (ЭТХ) (вектор $\mathbf{A}'_{\langle k'\rangle}\left(\mathbf{B}'_{\langle l'\rangle}\right)$) средств реализации сценария деструктивного воздействия (СДВ) виртуального злоумышленника, а также на характеристики (вектор $\mathbf{A}''_{\langle k''\rangle}\left(\mathbf{B}'_{\langle l'\rangle}\right)$) технологии (процесса организации) воздействия, проводимых этими средствами нападения, и через них обусловливающие возможные результаты $\mathbf{U}_{\langle 3\rangle} = \mathbf{U}_{\langle 3\rangle}(\mathbf{A}'_{\langle k'\rangle}, \mathbf{A}''_{\langle k''\rangle}; \mathbf{B}'_{\langle l'\rangle})$ этих воздействий. Вектор $\mathbf{U}_{\langle 3\rangle}$ характеризует потенциал компьютерного воздействия нарушителя — участника информационного конфликта в киберпространстве [1].

Применение средств воздействия происходит в условиях активного противодействия системы обнаружения вторжений (СОВ), характеристики которой обозначим через вектор $\mathbf{B}''_{\langle l''\rangle}$, влияющей на ситуацию и тем самым обусловливающей для нарушителя требуемые $\mathbf{U}^{\text{д}}_{\langle 3\rangle}\left(\mathbf{B}''_{\langle l''\rangle}\right)$ результаты реализации СДВ, т.е. $\mathbf{U}_{\langle 3\rangle} \in \left\{\mathbf{U}^{\text{д}}_{\langle 3\rangle}\right\}$ [2, 3].

Соотношение $\mathbf{U}_{\langle 3\rangle} \in \left\{\mathbf{U}^{\text{д}}_{\langle 3\rangle}\right\}$ представляет собой формальное выражение цели, в то время как содержательно цель определяется следующим образом: нарушение работоспособности объекта КИИ путем создания доминирующих в киберпространстве конфликтующих целенаправленных процессов (КЦП), или иначе — процессов нарушения информационной безопасности (ИБ).

Представленные выше векторы образуют так называемый операционный комплекс моделирования процессов нарушения ИБ, структура которого представлена в [3].

Таким образом, можно говорить о возникновении двуединой задачи, заключающейся, с одной стороны, в моделировании объектов КИИ как среды противоборства и функционирования СОВ — вектор $\mathbf{B}'_{\langle l'\rangle}$, с другой стороны, в моделировании киберпротивника $\mathbf{U}_{\langle 3\rangle}$, представленного в КИИ в виде КЦП (вектор $\mathbf{A}''_{\langle k''\rangle}$).

Анализ специфики построения и особенностей функционирования КИИ

Анализ специфики построения и особенностей функционирования КИИ в аспекте возможности моделирования СДВ злоумышленника и проектирования проактивных СОВ позволяет отнести объекты КИИ к сложным системам [3, 4]. Приведем характеристики $\mathbf{B}'_{\langle l'\rangle}$ (но не формальные признаки) этих объектов, характеризующих их как сложную систему.

1. Уникальность объекта. Объекты КИИ обладают уникальной структурой и индивидуальными особенностями своего функционирования. Как следствие, низкая возможность успешного применения нарушителем какой-либо типовой стандартной процедуры реализации СДВ. Это обстоятельство удорожает процедуру построения системы проведения информационно-технического воздействия и проактивной СОВ.

2. Сложность в четкой формализации цели функционирования объекта и критериев оптимального управления им. Для большинства объектов КИИ практически невозможно формализовать цель их функционирования. В результате нельзя математически четко задать критерии работоспособности объекта и критерии оптимального управления им. Как следствие, низкая возможность математического описания цели $\mathbf{U}_{\langle 3\rangle} \in \left\{\mathbf{U}^{\text{д}}_{\langle 3\rangle}\right\}$ воздействия в аспекте возможности нарушения работоспособности объекта КИИ, то есть невозможность математического формулирования критерия пригодности сценария деструктивного воздействия по его результатам (критерия, оценивающего качество результатов воздействия).

3. Нестационарность режима функционирования объекта КИИ. Заключается в эволюции числа и значений характеристик объекта во времени, когда с течением времени изменяется его структура и функционирование. Проявляется эта черта в различной реакции объекта на одну и ту же ситуацию или деструктивное воздействие в различные моменты времени. Поэтому при синтезе модели объекта КИИ необходимо вво-

дить ее динамичную коррекцию. Это создает серьезные трудности при синтезе модели воздействия на объект. Как следствие, проектируемые системы моделирования процесса реализации сценариев деструктивного воздействия должны быть адаптивными, готовыми к изменению своего функционирования.

4. Автоматизированная система. Обязательными элементами структуры объектов КИИ являются люди. В отличие от других элементов КИИ люди обладают свободой действий в рамках функционирования объекта и управления им с учетом своих личных интересов и целей. Вследствие этого их внешнее управление нарушает «нормальное» функционирование объекта, т.е. изменяет его самостоятельное поведение и делает зависимым от субъекта.

5. Неполнота описания объекта. Как правило, коллектив экспертов, знающих КИИ как предполагаемый объект воздействия, не в состоянии сразу же обеспечить полноту информации, которой бы заведомо хватило для создания системы воздействия. Это происходит по нескольким причинам.

Лицо, принимающее решение (ЛПР) на реализацию СДВ, из-за сложности объекта почти целиком полагается на экспертов, знающих этот объект. Тот или иной уровень допущений при описании КИИ фактически предлагают они. Но, не будучи специалистами по проведению информационно-технических воздействий, эксперты не могут оценить тот уровень полноты описания, который нужен специалисту по воздействию на объект КИИ.

Другая важная причина неполноты описания объекта — незнание некоторых сторон его функционирования самими экспертами. Примером является незнание правильной последовательности реализации атомарных событий информационной безопасности в структуре СДВ или, например, последовательности отказов элементов КИИ в процессе его реализации, выполнение которых может привести КИИ в аварийную ситуацию. В этом случае специалист не будет знать точный сценарий реализации деструктивного воздействия.

Третья причина неполноты описания — отсутствие у эксперта четкого понимания алгоритма функционирования объекта. Выдавая специалисту информацию об объекте, он в состоянии передать ЛПР интуитивные соображения, по которым сам принимает решение о функционировании объекта.

Еще одна причина, приводящая к неполноте описания сложных объектов, состоит в том, что многие особенности функционирования объекта, а иногда и структура и связи между элементами не могут быть описаны достаточно полно и точно. Они допускают лишь качественное, словесное описание. Переход от качественных описаний к некоторым формальным представлениям должен производиться специалистом по информационно-техническому воздействию, который не всегда в состоянии решить такую сложную проблему.

Постановка задачи априорного оценивания эффективности деструктивного воздействия виртуального злоумышленника

В результате на этапе внешнего проектирования облика проактивной СОВ и оценивания эффективности их применения возникают следующие актуальные задачи, предшествующие собственно задаче априорного оценивания эффективности деструктивного воздействия виртуального злоумышленника:

1. Задача математического обоснования показателя V целевого эффекта — результативности компьютерной атаки (КА) (т.е. результата, ради которого проводится КА). Показатель V является одной из компонент комплексного показателя потенциала нарушителя $\mathbf{U}_{\langle 3\rangle} =< V, R, T >$, где R — показатель ресурсоемкости деструктивного воздействия; T — показатель оперативности реализации СДВ [5].

2. Задача математического обоснования области $\left\{\hat{\mathbf{U}}^{\text{д}}_{\langle 3\rangle}\right\}$ допустимых значений возможных результатов $\hat{\mathbf{U}}_{\langle 3\rangle}$ реализации СДВ и критерия оценивания качества результатов реализации СДВ: $\hat{\mathbf{U}}_{\langle 3\rangle} \in \left\{\hat{\mathbf{U}}^{\text{д}}_{\langle 3\rangle}\right\}$ [6].

Такой подход позволяет сформулировать следующее утверждение: для математического моделирования методов воздействия на сложный объект КИИ необходимо создать адекватную математическую модель процесса функционирования данного объекта. Это утверждение распространяется и на киберпротивника, как сложного объекта исследования и воздействия.

В области ИБ задача построения адекватной математической модели сложного объекта защи-

ты в настоящее время полностью не решена. Более того, нет единой методологии разработки таких моделей в данной предметной области. Поясним данную проблемную ситуацию.

Традиционная теория автоматического управления техническими объектами исходит из положения, что любой объект управления (далее объект воздействия) может быть формально описан в виде достаточно простой математической модели. В качестве такой модели используются различного рода дифференциальные уравнения. В более сложных случаях модель может представлять собой систему интегро-дифференциальных уравнений или смешанную систему, в которую наряду с дифференциальными уравнениями входят алгебраические и другие уравнения, связывающие между собой параметры, описывающие структуру (процесс) функционирования объекта.

Формализация такого типа считается необходимым и достаточным условием поиска оптимального способа воздействия на объект, а возможность такой формализации всегда постулируется. Другими словами, задача воздействия априори считается формализованной, то есть в зависимости от вида уравнений, описывающих поведение объекта и системы воздействий на него, а также в зависимости от того критерия воздействия, который был задан, выбирается пригодный метод поиска оптимального воздействия. Данные методы поиска широко известны в традиционной теории управления (методы линейного программирования, динамического программирования и другие), а класс исследуемых в данной теории объектов принято называть простым [3].

Краткая классификация объектов КИИ

В соответствии с [7] под простым объектом понимается объект, для управления которым необходима и достаточна формальная теория объекта. Некоторые простые объекты управления могут не иметь математического описания, однако если простыми объектами можно управлять без их математической модели, то сложными уже нельзя.

К простым объектам следует отнести и так называемый класс сложных формализуемых систем, на которых остановимся подробнее. В разное время предлагались различные математические модели таких сложных систем: диагностируемая система Дмитриева А.К., Юсупова Р.М., агрегативная система Бусленко Н.П., непрерывно-дискретная система Глушкова В.М., гибридная система А. Пнуэли и многие другие [7–9].

Каждый из авторов предлагает свою модель и новый формальный подход к описанию, как они предполагают, нового класса сложных систем. Результат анализа показывает, что в действительности в этих трудах исследуются один и тот же класс динамических систем с переменной структурой, характерной для производственных процессов, для исследования которых не всегда пригодны классические методы прикладной математики — в этом и заключается «сложность» данных систем. Для моделирования их поведения и структуры используются формальные методы теории массового обслуживания, теории игр и статистических решений, теории автоматов, теории статистического моделирования и др., а сама автоматизированная система управления рассматривается как единая сложная система совместно с управляющими подсистемами. Делается попытка унификации структуры моделей на базе так называемых агрегативных систем, позволяющих с единой точки зрения описывать процессы различной природы.

Такие сложные динамические системы часто называют гибридными системами (что абсолютно правильно), поведение которых обусловлено совместным функционированием непрерывных и дискретных объектов, мгновенными качественными изменениями в непрерывном объекте, изменением состава системы.

Следует заметить, что в технической литературе часто используются термины «смешанная система», «агрегативная система», «непрерывно-дискретная система», «система с переменной структурой», «событийно-управляемая система», семантика которых не всегда понятна. Объективное исследование этого противоречия представлено в работе [5], результатами этого анализа является доказательство приводимости различных математических моделей сложных систем друг к другу. На основании этого может быть сделан вывод о том, что представленные выше термины являются синонимами и описывают один класс простых объектов.

Традиционная схема управления простыми объектами представлена на рис. 1.

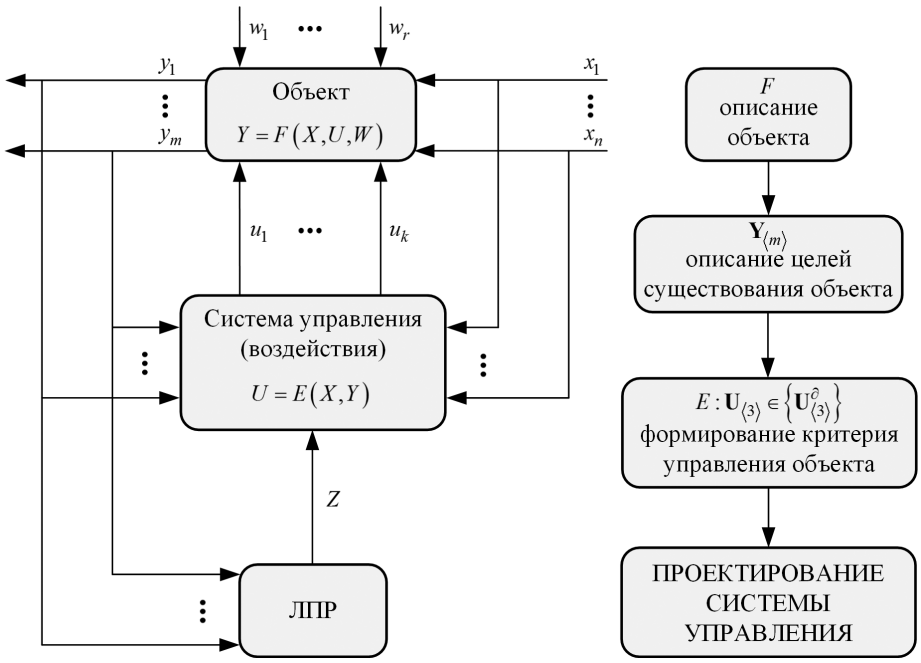

Рис. 1. Традиционная схема управления простыми объектами

В соответствии с рис. 1 для моделирования системы воздействия на объект требуется определить множество предпочтительных векторов $\mathbf{Y}_{\langle m \rangle}$ и отображение F. Отображение F описывает специфику построения и особенности функционирования объекта воздействия, а знание предпочтительных значений $\mathbf{Y}_{\langle m \rangle}$ говорит о понимании цели его функционирования. Эти сведения позволяют сформулировать критерий E оптимального воздействия на объект, $E : \mathbf{U}_{\langle 3 \rangle} \in \left\{ \mathbf{U}^{\text{д}}_{\langle 3 \rangle} \right\}$. Критерий E может быть различным, но именно наличие критерия воздействия позволяет ставить и решать традиционную задачу проектирования системы управления простым объектом.

Традиционная схема проектирования системы воздействия на простые объекты имеет ряд ограничений. Как правило, специалисты прилагали усилия лишь к поиску процедуры управления объектом, когда F, $\mathbf{Y}_{\langle m \rangle}$, E были уже описаны в точных терминах. То есть простой объект воздействия, как правило, заменялся некоторой синтаксической формальной моделью — некоторым уравнением. Далее независимо от семантики решаемой задачи применялись различные методы нахождения оптимального управления. По сути, простой объект синтаксически формализуем и моделируется конечным автоматом с дискретным временем либо, в случае гибридных систем, гибридным автоматом с различными моделями непрерывного времени, а сама конструкция автомата предопределяется двумя свойствами объекта управления — его полной управляемостью и идентифицируемостью.

Для управления сложными объектами формальная синтаксическая модель объекта не применима. Действительно, как объект КИИ, так и киберпротивник — это неидентифицируемые и трудно управляемые объекты воздействия. Отсюда возникает проблема идентификации этих сложных информационных объектов и проблема выявления критериев оптимального управления ими. Как следствие, все трудности воздействия определяются сложностью объекта, поэтому следует начинать именно с моделирования объекта, а не с алгоритма управления им.

Рассмотрим в самом общем виде постановку задачи воздействия на сложный информационный объект. Текущей ситуацией на объекте воздействия будем называть совокупность всех сведений о структуре объекта воздействия и его функционировании в данный момент времени. Полной ситуацией будем называть совокупность, состоящую из текущей ситуации, знаний о состоянии системы воздействия в данный момент и знаний о технологии воздействия. Обозначим полные ситуации через S_i, а текущие ситуации через Q_j. Пусть в распоряжении системы воздействия имеется n различных способов

воздействия на объект атаки — одношаговых решений U_k. Элементарный акт воздействия можно представить в следующем виде — $S_i; Q_j \underset{U_k}{\Rightarrow} Q_l$.

Физический смысл этого соотношения заключается в следующем. Если на объекте воздействия сложилась ситуация Q_j и состояние системы воздействия, определяемое S_i, допускает использование воздействия U_k, то оно применяется. Текущая ситуация Q_j превращается в новую ситуацию Q_l. Подобные правила преобразования будем называть логическими правилами (ЛП), а их список задает возможности системы воздействия влиять на процессы, протекающие в объекте. Данная постановка задачи воздействия на сложный объект основана на введении понятия ситуации, классификации ситуации и их преобразовании. Методы воздействия в рамках данной постановки задачи будем называть методами ситуационного воздействия по аналогии с методом ситуационного управления [10].

Принципы семиотического моделирования СОВ

Под формальной моделью будем понимать четверку $M = T, P, A, \Pi$, где T — множество базовых элементов; P — синтаксические правила; A — система аксиом; П — семантические правила. В синтаксических системах, описывающих простые объекты, T, P, A, П остаются неизменными. Это означает, что если бы формальные системы использовались для создания ситуационных моделей воздействий на сложные объекты, то язык описания ситуаций (он определяется T и P), исходные знания об объекте воздействия и законах воздействия (они определяются заданием множества аксиом A) и ЛП (они совпадают с семантическими правилами П) оставались бы неизменными.

Как видно, это противоречит характерным чертам сложных объектов, так как система воздействия на них, базирующаяся на формальной синтаксической модели и моделируемая автоматом, априорно должна иметь всю информацию, которая остается для нее неизменной в течение всего периода воздействия. Теорию автоматов, лежащую в основе большинства современных кибернетических устройств, еще называют стимульно-реактивной теорией [10, 11] автоматов в силу того огромного значения, которое играет для этой теории психологическая схема «стимул-реакция».

Однако следует признать, что моделирующие возможности современных автоматов все еще невысоки. Так, не вполне удачны предпринимаемые в кибернетике попытки смоделировать с помощью стимульно-реактивных устройств процесс принятия решения человеком. Характерны в этом отношении неудачи так называемого эвристического программирования, используемого в технологии проактивной защиты. В области ИБ примерами стимульно-реактивных устройств являются антивирусные средства, системы обнаружения атак и другие средства, в основе функционирования которых заложена реактивная (сигнатурная) технология, недостаток которой очевиден.

Уникальность сложного объекта требует для описания его структуры, функционирования и особенностей поведения специальных семантических и прагматических формальных моделей. Это требует специальных языковых средств для описания таких моделей. К сожалению, классическая математика не позволяет сделать это. Выход из создавшейся проблемной ситуации видится в применении методов ситуационного управления и семиотического моделирования, разработанных в рамках прикладной семиотики [11].

В прикладной семиотике одно из центральных мест занимает понятие семиотического моделирования. Суть семиотического моделирования заключается в следующем. В процессе функционирования системы воздействия на сложные объекты могут корректироваться языки описания ситуаций, изменяться знания об объекте и методах воздействия на него. Это означает, что все элементы, входящие в определение формальной синтаксической модели M, могут изменяться в процессе ее функционирования. С этой целью рассматривается семиотическая модель вида $C =< M, \chi_T, \chi_P, \chi_A, \chi_\Pi >$, предложенная Поспеловым Д.А. Здесь $\chi_T, \chi_P, \chi_A, \chi_\Pi$ — соответственно, правила изменения T, P, A, П. Правила χ_T, χ_P меняют синтаксис базовых элементов и их совокупностей, правила χ_A, χ_Π — семантику и прагматику этих совокупностей.

Раскроем физический смысл элементов семиотической модели точнее. Модель M детерминирована и неизменна. Правила χ_Π

дают возможность отказаться от этого, сделать ЛП переменными, например, адаптивными. Примерами таких ЛП могут служить ЛП с вероятностной перенастройкой вида $S_i;Q_j \underset{U_k}{\Rightarrow}(Q_{l1},q_1;Q_{l2},q_2;...;Q_{lr},q_r)$. В таком ЛП текущая ситуация Q_j при полной ситуации S_i преобразуется не в одну фиксированную текущую ситуацию Q_l, как было ранее, а в r различных текущих ситуаций. Выбор того или иного преобразования осуществляется вероятностным механизмом q_i. В зависимости от удачи или неудачи применения такого ЛП происходит изменение распределения. Такой способ ЛП позволяет подстраивать семантические правила под тот объект, для которого построена система воздействия.

Знания об объекте, его состоянии, а также состоянии системы воздействия можно выразить в виде набора аксиом χ_A. Они служат источником вывода о том воздействии U_k^*, которое необходимо применить в данном случае. В другой момент времени t+1 эти знания будут уже другими. Например, было обновлено программное обеспечение на некоторых хостах компьютерной сети, и реализация воздействии $U_k^*(t+1)$ будет неудачным. Поэтому система аксиом должна адекватно меняться с учетом изменений предметной области. Эти изменения можно явно указывать, например, в правых частях ЛП, записывая их в виде $S_i;Q_j \underset{U_k}{\Rightarrow}Q_l;I_i$. Здесь I_i — те изменения аксиом, задаваемых правилами χ_A, которые необходимо внести в описание полной ситуации S_i после перехода Q_j в Q_l.

Изменения синтаксических правил могут свидетельствовать, что язык описания ситуаций на объекте, полные знания о нем и процедурах воздействия оказался слишком «бедным». Например, в зависимости от текущей ситуации, возникает необходимость использовать разные модели представления объектов КИИ, например, теоретико-множественная модель, модель в виде древовидной (иерархической) структуры, модель в виде семантической сети структуры. Функции такого изменения выполняют правила χ_P. Правила χ_T добавляют в список исходных знаний об объекте новые элементы или исключают из него те, которые оказались ненужными для целей воздействия.

Семиотическую модель системы воздействия на сложный объект (или семиотическую модель целеустремленной конфликтующей системы или систему воздействия, базирующуюся на семиотической модели) можно представить в виде сети, показанной на рис. 2.

Каждая вершина сети есть некоторая формальная синтаксическая система M^i, связи между вершинами есть переходы от одной системы M^i к другой под влиянием изменений χ^i. Эти изменения могут совпадать с $\chi_T,\chi_P,\chi_A,\chi_\Pi$ или быть какой-то их комбинацией. За один такт ра-

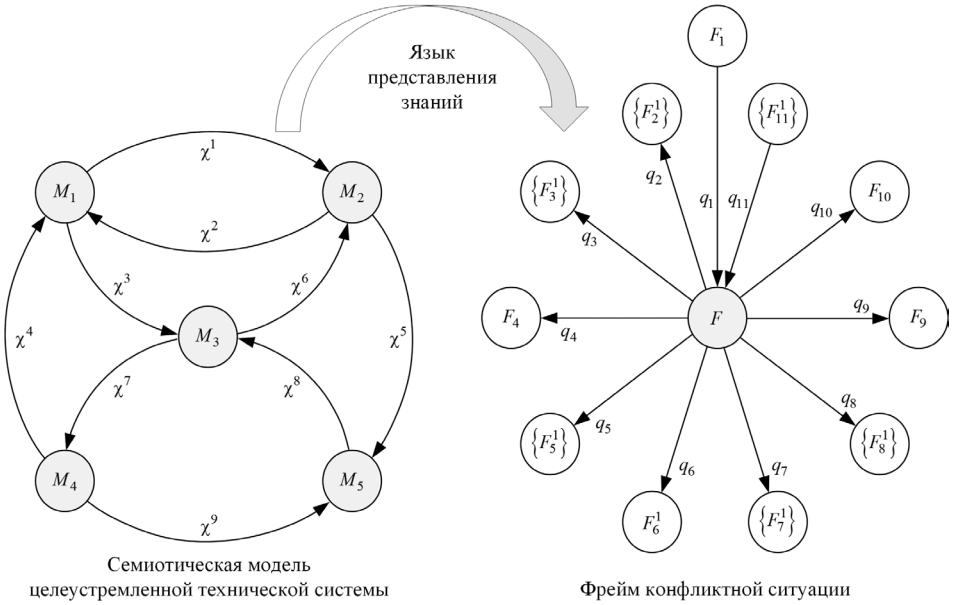

Рис. 2. Пример типовой семиотической модели СОВ

боты семиотической модели в зависимости от содержимого I_i модель либо останется в том же состоянии (в рамках той же формальной системы), что и ранее, либо перейдет в новое состояние.

В качестве языка для описания текущих и полных ситуаций, характеризующих объект воздействия и систему воздействия, можно использовать язык ситуационного управления, язык RX-кодов, язык исчисления предикатов первого порядка, универсальный семантический код и другие.

Представленные выше логические языки описания конфликтных ситуаций требуется преобразовать в специальные языки представления знаний для организации удобной машинной обработки. В качестве моделей представления знаний предлагается использовать фреймовые модели (рис. 2), типовое описание фрейма конфликтной ситуации будет представлено ниже.

Каждый фрейм должен представлять готовую структуру, которая при том или ином заполнении слотов значениями превращается в описание конкретной конфликтной ситуации. Фреймы-прототипы должны хранить знания о предметной области, а конкретные фреймы пополнять эти единицы знания реальными данными. Это позволит классифицировать различные конфликтные ситуации, описать способы их обнаружения, и, как следствие, предложить способы устранения конфликтных ситуаций.

Пример. F — фрейм-прототип, F_1 — фрейм хранения конкретных данных о возникшем конфликте, например, данные о возможном потенциале $\mathbf{U}_{\langle 3\rangle}$ нарушителя. Эти данные используются во фрейме F для понимания целостной картины конфликта и выбора модели, пригодной для исследования нарушителя.

Множество $\{F_2^i\}$ — фреймы, которые требуется анализировать при возникновении конфликта, описанного во фрейме F_1. Множество $\{F_3^i\}$ содержит фреймы, в которых содержится информация, характеризующая тот класс конфликтных ситуаций, к которому принадлежит ситуация, составляющая значение слотов в F_1.

В качестве примера можно привести детерминированные, стохастические и неопределенные ситуации, возникающие в процессе моделирования нарушителя и его воздействий.

Множества $\{F_5^i\} - \{F_8^i\}$ — множества фреймов, в которых содержатся способы устранения конфликта, возникшего, например, при нарушении работы структурных подразделений на объекте защите, при отклонениях показателей штатного процесса функционирования, при анализе журналов аудита ИБ.

В фрейме F_9 может формироваться оценка степени конфликтности возникшей ситуации. Фрейм F_{10} фиксирует динамику развития конфликтной ситуации, хранит те мероприятия, которые уже были применены для уменьшении степени конфликтности ситуации.

Наконец, множество фреймов $\{F_{11}^i\}$ хранит информацию, необходимую для анализа причин возникновения конфликтной ситуации. Движение по всем связям q_i, показанным на рис. 2, происходит за счет процедуры, которая хранится во фрейме-прототипе F.

Заключение

Таким образом, учитывая выше сказанное, следует заключить, что в основе внешнего проектирования проактивных систем ИБ должна лежать концепция семиотического моделирования и ситуационного управления сложными объектами. В статье был раскрыт принцип рефлексивного управления нарушителем ИБ, который совместно с методами прикладной семиотики должны составлять существо «проактивности» проектируемых современных СОВ.

Литература

1. Сухов А.М., Крупенин А.В., Якунин В.И. Методы анализа и синтеза исследования эффективности процессов функционирования системы обнаружения предупреждения и ликвидации последствий компьютерных атак // Автоматизация процессов управления. 2021. № 4 (66). С. 4–14.

2. Диченко С.А., Финько О.А. Контроль и восстановление целостности многомерных массивов данных посредством криптокодовых конструкций // Программирование. 2021. № 6. С. 3–15.

3. Петухов Г.Б., Якунин В.И. Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем. — М.: АСТ, 2006. 503 с.

4. Диченко С.А. Модель угроз безопасности информации защищенных информационно-аналитических систем специального назначения //

Вопросы оборонной техники. Серия 16. Технические средства противодействия терроризму. 2022. № 1–2 (163–164). С. 64–71.

5. Сухов А.М. Подход к упреждению комплексных компьютерных атак в автоматизированной системе специального назначения // Труды Военно-космической академии им. А.Ф. Можайского. 2017. № 658. С. 62–77.

6. Сухов А.М., Герасимов С.Ю., Еремеев М.А. и др. Математическая модель процесса функционирования подсистемы реагирования системы обнаружения, предупреждения и ликвидации последствий компьютерных атак // Проблемы информационной безопасности. Компьютерные системы. 2019. № 2. С. 56–64.

7. Дмитриев А.К., Юсупов Р.М. Идентификация и техническая диагностика. — М.: МО СССР, 1987. 521 с.

8. Бусленко Н.П. Моделирование сложных систем. — М.: «Наука», 1978. 399 с.

9. Глушков В.М. Программное обеспечение моделирования непрерывно-дискретных систем. — М.: «Наука», 1975. 236 с.

10. Юсупов Р.М., Петухов Г.Б. и др. Статистические методы обработки результатов наблюдений. — М.: МО СССР, 1984. 563 с.

11. Поспелов Д.А. Ситуационное управление: теория и практика. — М.: Наука, 1986. 288 с.

References

1. Sukhov A.M., Krupenin A.V., Yakunin V.I. Methods of analysis and synthesis of research into the effectiveness of the functioning of the system of detection, prevention and elimination of consequences of computer attacks // Automation of control processes. 2021. № 4 (66). P. 4–14.

2. Dichenko S.A., Finko O.A. Control and restoration of the integrity of multidimensional data arrays by means of crypto code constructions // Programming. 2021. № 6. P. 3–15.

3. Petukhov G.B., Yakunin V.I. Methodological foundations of external design of purposeful processes and purposeful systems. — M.: AST, 2006. 503 p.

4. Dichenko S.A. Model of information security threats of protected information and analytical systems of special purpose // Voprosy oboronnoi tekhniki. Seriia 16. Tekhnicheskie sredstva protivodestviia terrorizmu. 2022. № 1–2 (163–164). P. 64–71.

5. Sukhov A.M. Approach to the prevention of complex computer attacks in a special purpose automated system // Proceedings of the Military Space Academy named after A.F. Mozhaisky. 2017. № 658. P. 62–77.

6. Sukhov A.M., Gerasimov S.Yu., Eremeev M.A. et al. Mathematical model of the process of functioning of the response subsystem of the system for detecting, preventing and eliminating the consequences of computer attacks // Problems of information security. Computer systems. 2019. № 2. P. 56–64.

7. Dmitriev A.K., Yusupov R.M. Identification and technical diagnostics. — M.: Ministry of Defense of the USSR, 1987. 521 p.

8. Buslenko N.P. Modeling of complex systems. — M.: «Science», 1978. 399 p.

9. Glushkov V.M. Software for modeling continuous-discrete systems. — M.: «Science», 1975. 236 p.

10. Yusupov R.M., Petukhov G.B. et al. Statistical methods of processing the results of observations. — M.: Ministry of Defense of the USSR, 1984. 563 p.

11. Pospelov D.A. Situational management: theory and practice. — M.: Nauka, 1986. 288 p.