МОДЕЛЬ СИСТЕМАТИЗАЦИИ КЛАССИФИКАТОРОВ ДЕСТРУКТИВНЫХ И КОНСТРУКТИВНЫХ СОБЫТИЙ ЦИФРОВОГО ПРОСТРАНСТВА

Рыженко А. А.[1], Селезнёв В. М.[2]

DOI: 10.21681/2311-3456-2024-3-113-119

Целью работы *является разработка обобщенной формальной модели систематизации основных классификаторов деструктивных и конструктивных событий инфраструктуры цифрового пространства суверенного государства для организации автономности интеллектуального агента в форме фасета данных.*

Метод исследования: *использование синтаксического представления данных теории информации на стыке модели управления сложными системами и модели информационной безопасности для формализации в виде концептуальной модели.*

Результат исследования: *разработана обобщенная модель систематизации классификаторов деструктивных и конструктивных событий противоборствующей системы в пределах цифрового пространства суверенного государства, позволяющей не только использовать собственные ресурсы для прогнозирования атак и устранения деструктивных элементов на программном уровне, но и привлекать цифровой образ социальной среды как одного из основных элементов для решения задач. В качестве связующего звена в работе предложено использовать интеллектуальных агентов бот-сети, функционал которых предполагает не только теневое взаимодействие с пользовательскими рабочими местами, но и работой с социальной средой непосредственно. Полученная постановка решает актуальную проблему формализации данных – моделирование процессов противодействия внешним деструктивным атакам с распределением функциональных задач, что позволит пересмотреть концепцию собственной безопасности, увеличить стойкость цифровой среды к вероятным негативным воздействиям.*

Научная новизна *заключается в разработке нового элемента концептуального моделирования деструкторов в виде автономных моделей – фасетно-атрибутивного процесса, позволяющего не только адаптивно изменять правила перехода состояний, но и модифицировать собственные параметрические показатели.*

Ключевые слова: *деструктор, моделирование, интеллектуальный агент, фасет, иерархия, правила перехода, автоном, цифровое пространство, система.*

MODEL OF SYSTEMATIZATION CLASSIFIERS OF DESTRUCTIVE AND CONSTRUCTIVE EVENTS IN THE DIGITAL SPACE

Ryzhenko A. A.[3], Seleznev V. M.[4]

The aim of the work *is to develop a generalized formal model for systematizing the main classifiers of destructive and constructive events in the infrastructure of the digital space of a sovereign state to organize the autonomy of an intelligent agent in the form of a data facet.*

Research method: *using a syntactic representation of information theory data at the intersection of a model for managing complex systems and an information security model for formalization in the form of a conceptual model.*

Research result: *a generalized model for systematizing classifiers of destructive and constructive events of an opposing system within the digital space of a sovereign state has been developed, which allows not only to use its own resources to predict attacks and eliminate destructive elements at the program level, but also*

1 Рыженко Алексей Алексеевич, кандидат технических наук, доцент, доцент кафедры информационной безопасности, Финансовый университет при Правительстве РФ, г. Москва, Россия. E-mail: AARyzhenko@fa.ru

2 Селезнёв Владимир Михайлович, кандидат технических наук, заведующий кафедрой информационной безопасности, Финансовый университет при Правительстве РФ, г. Москва, Россия. E-mail: VMSeleznyov@fa.ru

3 Aleksey A. Ryzhenko, Ph.D., Associate Professor, Financial University under the Government of the Russian Federation, Moscow. E-mail: AARyzhenko@fa.ru

4 Vladimir Seleznev, Ph.D., Head of department of information security, Financial University under the Government of the Russian Federation, Moscow. E-mail: VMSeleznyov@fa.ru

to involve the digital image of the social environment as one of the main elements to solve problems. As a connecting link in the work, it is proposed to use intelligent botnet agents, the functionality of which involves not only shadow interaction with user workstations, but also work with the social environment directly. The resulting formulation solves the pressing problem of data formalization - modeling the processes of countering external destructive attacks with the distribution of functional tasks, which will allow us to reconsider the concept of our own security and increase the resistance of the digital environment to possible negative impacts.

***The scientific novelty** lies in the development of a new element of conceptual modeling of destructors in the form of autonomous models – a facet-attributive process, which allows not only to adaptively change the rules of state transition, but also to modify one's own parametric indicators.*

***Keywords:** destructor, modeling, intelligent agent, facet, hierarchy, transition rules, autonomy, digital space, system.*

Введение

Анализ многолетней статистики атак на цифровое пространство организаций и предприятий разного уровня и профиля выявил достаточно формализуемые закономерности, связанные с разными профессиональными категориями социальной среды. Здесь сразу необходимо сделать акцент, что описательных публикаций, содержащих разные аспекты и классификаторы объектов и процессов цифрового пространства в пределах одного государства достаточно много. В частности, можно выделить классификаторы, сопоставимые с направлениями деятельности или с группами документооборота и делопроизводства организаций. Дальнейший синтез и агрегация привели к более укрупненным классам по ключевым позициям: территориальная принадлежность, зональность по видам финансово-денежных отношений, границы в социальной среде и т.д. Каждый укрупненный класс в настоящее время уже имеет достаточно теоретических и практических наработок, позволяющих систематизировать потоковые данные всемирной цифровой среды, ограничивать доступ к информационным ресурсам, публикуемым в разрез с позицией государства (что также отражено в ряде нормативной документации международного уровня, например, «Право на забвение»). Дальнейшее объединение укрупненных классов не привела бы к положительным результатам, в результате, для данных выделенных классов с одной стороны начали образовываться научные школы (что также отражено во многих публикациях), с другой – на практике многие теоретические подходы нашли свое применение. Например, по линии ФСТЭК России такие достаточно сложные документы как модели угроз в организациях вобрали в себя многолетний опыт типов защит от атак. Но также есть и третья сторона, усложняющая процесс внедрения современных формальных моделей на практике – несостыковка позиций основных критериев в обычной среде и в цифровой. Например, территориальную принадлежность государства можно отобразить на географических и политических картах, а границы суверенного государства в цифровом пространстве определить с заданной точностью практически невозможно. Также стоит учесть, что за последние десятилетия основной акцент актуализации методов защиты информации все больше склоняется к границам в социальной среде, что непосредственно связано с массовым развитием методов негативного воздействия социальной инженерии[5]. Как следствие, дальнейшая формализация метода систематизации классификаторов деструктивных и конструктивных событий будет рассматриваться только как новая форма защиты от современных методов воздействия на социальную среду. Здесь необходимо сделать также и второй небольшой акцент – не совсем понятная тенденция отказа во многих публикациях изучать хронологию становления теоретических основ систем безопасности, основанных на практических результатах более чем десятилетней давности. Уже можно отметить ряд последствий, попадающих под «все новое – это хорошо забытое старое» и «лучшее – враг хорошего». В данной публикации в краткой описательной форме представлен результат анализа, как пример необходимости изучать истоки на примерах положительных достижений.

За последние уже 14 лет электронные издания все чаще публикуют результаты независимых классификаций, а также способов и подходов применения исторически устоявшихся психологических методологий воздействия на массовой сознание социума. Развитие современных информационных систем и технологий способствовало формированию принципиально новых методов воздействия, сочетавшие модели массового влияния, но с учетом персонификации каждого объекта воздействия в индивидуальном порядке. Устоявшиеся за последние 24 года

5 Социальная инженерия: анализ и методы противодействия. – режим доступа: https://cisoclub.ru/socialnaja-inzhenerija-analiz-i-metody-protivodejstvija/

методы последовательного воздействия на группы субъектов с целью достижения конкретной цели стало одним из основных направлений социальной инженерии. Например, телефонное мошенничество, «основанное» и описанное Кевином Митником в известном издании «Искусство обмана» [1]. Так широко разрекламированный в 90-е годы данный тип мошенничества развился в корпоративное мошенничество, появились новые формы воздействия на организации с использованием четко сформированных сценариев, алгоритмов и прочих последовательных этапов выполнения целевых задач. Массовые атаки на информационные ресурсы организаций, как правило, готовятся месяцы. Основные объекты предварительных (подготовительных) атак – простые сотрудники организаций, имеющие доступ к базам данных и прочей документации систем документооборота. С одной стороны, данная тенденция роста деструктивных воздействий должна волновать исключительно атакуемые объекты, с другой – явная тенденция последних лет массовой переориентации атак на критически важные объекты государственного уровня уже преподносит негативные последствия и недвусмысленно намекает на активное внедрение новых форм противоборства.

В результате многолетнего всестороннего анализа исторических фактов получено множество зависимостей прямых сценариев «*причина – фактор – сценарии*» и обратных «*цель – задачи – сценарии*». Появилась возможность формирования семантических связей, позволяющих автоматизировать процесс перехвата злоумышленников на разных этапах воздействия на социальную среду уровня цифрового пространства. Например, использование на практике разных методов доступа к конфиденциальной информации позволило сделать базу правил действий (в том числе и для разрабатываемого интеллектуального агента фишинговой системы) [2]. Применяя доступные каналы доступа к информации (социальные сети, мессенджеры, чаты и т.д.) агент собирает информацию о сотрудниках, создает информационные суррогаты биоинформации, готовит сценарии атак на информацию организаций с использование аппаратных и программных ресурсов сотрудников данных организаций (пассивные агенты).

Особенностью данной работы является разработанная модель обратной задачи элемента бот-сети, а также алгоритм адаптивного внедрения в действующую информационную систему без ущерба основному жизненному циклу как самой системы, так и окружающей цифровой среды (пространства) – интеллектуального агента в форме самостоятельно модифицируемого деструктора в условиях частичной анонимности.

1. Предыстория и связанная с этим работа

У данной модели, как и у множества аналогичных, достаточно продолжительная история с неоднозначными путями развития. Одним из ключевых исторических моментов стал учет юридического опыта многих государств с целью выявления базовых сценариев противоборства компьютерным атакам на социальную среду. Например, в работе[6] автор рассматривает ряд вопросов, заложивших пути дальнейшего развития такого важного направления, как самозащита в организованных сетях, где социум мог (на тот момент времени) дистанционно общаться по разным вопросам на расстоянии без очного участия. В продолжении данного материала хочется отметить работу[7], где автор приводит альтернативные точки зрения на методологии судебных компьютерных исследований. Данный фактор вызван существенными изменениями даже на тот момент в сфере компьютерных преступлений с использованием сетей общего доступа. В России данный период ознаменовался вступлением в силу первых достаточно серьезных статей уголовного кодекса, предполагающих наказание за совершенные преступления в цифровой среде.

Необходимо отметить, что преступный мир не стоял на месте и развивался в 2000-х годах намного быстрее, чем могли себе это представить правоохранительные органы того времени. Например, достаточно известное эссе прародителя всемирной сети Интернет Билла Джоя в 2000 году заложило принципиального новое направление в сфере деструкторов – *метаморфы* и *полиморфы*. Особенностью данных конструкций была возможность саморазвития за счет использования трех практически независимых составных частей: голова, тело и хвост. Достаточно серьезные исследования возможного противоборства данной разновидности деструкторов приводили к одной общей мысли: *уничтожить данный вид деструктора практически невозможно, а проводить аудит действий и прогнозировать возможные негативные процессы вполне возможно*.

Тем не менее, благодаря первому полученному уже многолетнему опыту менялись сценарии противоборства, модифицировались алгоритмы и методики, о чем было отмечено во множестве публикаций. На тот момент многие разработчики уже задумались о возможности использовать дополнительные встроенные модули в систему обозревателей Интернет, позволяющие использовать антифишинговые

6 Bénichou, D., Lefranc, S. Introduction to Network Self-defense: technical and judicial issues. J Comput Virol 1, 24-31 (2005). https://doi.org/10.1007/s11416-005-0006-5

7 Broucek, V., Turner, P. Winning the Battles, Losing the War? Rethinking Methodology for Forensic Computing Research. J Comput Virol 2, 3-12 (2006). https://doi.org/10.1007/s11416-006-0018-9

панели с использованием функционала *cookies*, что применяется и по настоящее время[8].

Следующий год был ознаменован тем, что данный тип деструкторов перешел на новый уровень, появилась новая функция, предполагающая размножение вирусов в полуавтономном режиме. Также деструкторы научились скрывать свои тела в других программах как часть кода, и в других процессах доверенной зоны, а две другие составляющие (голова и хвост) стали независимы друг от друга, но вполне объединяющиеся при обнаруживании в пределах одной системы. Описанные процессы и множество других негативных факторов отмечены в ряде работ[9].

В 2010 году разработчики методов и моделей противоборства вирусным атакам обратили внимание на интеллектуальные системы, способные, как и вирусы *полиморфики*, самостоятельно развиваться в полуавтономном режиме. Многие публикации того времени отразили приоритетные направления исследований, а также предполагаемые результаты. Необходимо сразу отметить, что прогнозы десятилетней давности сбылись и уже применяются на практике. Например, авторами представлен новый метод интеллектуального анализа данных и пример использования нейронных сетей для обнаружения определенного типа деструкторов[10]. Также не забыты и классические методы, показавшие свою эффективность и в других направлениях моделирования. При этом исследования процессов новых модификаций деструкторов продолжились, получая все новые результаты.

В 2013 году исследователи обратили внимание в существенное изменений вирусов метаморфов. Новые энтропийные функции позволяли вносить некоторую избыточность в тело, что позволяло активировать новый функционал встроенного самоконтроля. Благодаря новой технологии метаморфы могли прятаться и становиться псевдонимны. Данный процесс стали позже использовать при хранении персональных данных. Эксперты также провели достаточно интересное исследование, позволяющее дать однозначную оценку в возможных путях развития вредоносных деструкторов, а также предполагаемые механизмы обнаружения. Естественным развитием стало внедрение модифицированной технологии обнаружения новой формы вирусных атак. Исследование результатов деятельности внедренных интеллектуальных агентов позволили выявить структуры новой формы метаморфа, что позволило в последующем разработать новые инструменты противоборства[11].

На данном этапе развития противоборства в цифровой среде можно выделить новую особенность, связанную с перенаправлением части исследовательских ресурсов в сторону защиты от новых методов социальной инженерии, напрямую связанных с деятельности вредоносного полиморфного вируса. Многими исследователями отмечено, что классическая форма прямой атаки на социум, с использованием сети Интернет стало частью прошлого. Современные полуавтономные сети модифицирующихся вирусов, собирающие данные о пользователях как части общей системы – новый опасный фактор. Как следствие, текущий анализ целевых атак на организации должен быть более комплексным с учетом возможных вариаций и альтернативных вариантов решений. Новые исследования в данном направлении привнесли в существующие алгоритмы достаточно эффективные методы выбора альтернатив сценариев противоборства метаморфам с учетом опыта многолетних ошибок. Например, ошибок в существующем программном обеспечении[12].

Развитие интеллектуальных систем не стояло на месте и продолжало развиваться в разных направлениях противоборствующих систем. Например, интересный подход обнаружения скрытых атак в потоке информации, описанный в [3], а также возможность использования результатов исследований, способствовали выделению в последующих исследованиях нескольких типов вредоносного программного обеспечения. Также получило развитие направление выявления скрытых угроз как для полиморфов, так и для метаморфов. В результате, можно отметить совершенствование существующих моделей злоумышленник / защитник для обучения кибербезопасности интеллектуальных моделей, в том числе и моделей противоборства социальной инженерии [4].

В 2020 году разработанный ранее подход противоборства видоизменяющимся вирусным атакам получил системный подход, о чем было отмечено в работе [5]. Разрабатываемые на основе новых моделей семантические алгоритмы нейронных сетей, способных выявлять формирование бот-сетей на разных этапах положили новое направление исследований, где роль интеллектуальных агентов стала иметь важное значение [6]. Также хочется отметить, что развитие моделей раннего обнаружения негативного фактора, приводящего к деструктивным

8 Li, L., Helenius, M. Usability evaluation of anti-phishing toolbars. J Comput Virol 3, 163–184 (2007). https://doi.org/10.1007/s11416-007-0050-4

9 Jacob, G., Filiol, E. & Debar, H. Functional polymorphic engines: formalisation, implementation and use cases. J Comput Virol 5, 247-261 (2009). https://doi.org/10.1007/s11416-008-0095-z

10 El-Bakry, H.M. Fast virus detection by using high speed time delay neural networks. J Comput Virol 6, 115-122 (2010). https://doi.org/10.1007/s11416-009-0120-x

11 Mezzour, G., Carley, L.R. & Carley, K.M. Longitudinal analysis of a large corpus of cyber threat descriptions. J Comput Virol Hack Tech 12, 11-22 (2016). https://doi.org/10.1007/s11416-014-0217-8

12 Tripathi, N., Hubballi, N. Detecting stealth DHCP starvation attack using machine learning approach. J Comput Virol Hack Tech 14, 233-244 (2018). https://doi.org/10.1007/s11416-017-0310-x

последствиях, стало широко использоваться и в социальных сетях [7].

Развитие не стоит на месте и продолжает совершенствоваться. За последующие 2 года получены достаточно интересные результаты в плане исследований внутренних процессов метаморфов с целью раннего прогнозирования возможных деструктивных действий на социальную среду [8].

С другой стороны, многолетний анализ приводит к неоднозначному выводу несуществования единой модели противоборства как самим проявлениям полиморфа и метаморфа, так и адаптивной бот-сети, состоящей из нестабильных интеллектуальных агентов. Также данному обстоятельству способствует быстро развивающееся направление анонимизации агентов, хранящих в себе саморазвивающиеся процедурные алгоритмы. Как следствие, в данной работе предлагается рассмотреть процессную модель формирования правил выбора альтернативных решений с множественным решением. Данная технология достаточно хорошо показала себя на практике при разрешении коллизий разного уровня в достаточно плотном пространстве, т.е. при множественном анализе системы и как целое, и как множество несвязанных автономов одновременно.

2. Новый подход формализации данных, основанный на алгебре процессов

В качестве схемы организации данных первичной обработки для построения сценариев, как было представлено ранее, например [9], используем:

- *базу правил развития событий* (обратное дерево решений) на основе сформированных алгоритмов многолетнего опыта исследователей для определения сценариев атак с использованием разветвленных альтернативных решений, представленных по ссылкам на публикации в предыдущей части данной статьи. Например, публикации по выявлению атак в социальных сетях позволили сформировать базовые правила подготовительного и начального этапов;
- *базы ассоциаций*, позволяющие порождать интеллектуальных агентов (прямое дерево решений) под конкретные задачи и хранящие целевое предназначение каждого агента в пассивном, теневом режиме вплоть до активной фазы. Например, при краже личности и формировании цифрового образа человека первым этапом является анализ социальной сети и сетевой активности в известных мессенджерах. Порождаются (формируется однозадачный код) агенты выполняющие четко определенные задачи поиска в определенное время (по таймеру или будильнику). Как правило такие агенты закладываются на независимые ресурсы всемирной сети в анонимной форме.

Вариант построения деревьев рассмотрен при моделировании системы организации данных бот-сети [10]. Далее процесс моделирования разбит на две последовательные части:

1) моделирование процессов перехода состояний по ветвям деревьев в условиях множественного выбора и множества решений;
2) моделирование системы организации данных адаптивных моделей бот-сетей в условиях начальной неопределенности.

3. Моделирование системы организации процессов многокритериальной модели дискретного пространства данных

Как уже было упомянуто ранее, анализ исходных формальных моделей, приведенных в первой части статьи позволил сформировать связи между конструктивной частью системы и деструктивной в виде продукционных правил в алгебраической форме. Особенности построения правил в системе процессов алгебры мультимножеств расшифрованы в публикациях, где приведен анализ процесса обработки данных систем документооборота для организаций финансового сектора и промышленной среды, а также формам формализации систем поддержки управления [11]. Дальнейшее моделирование потребовало увязать несколько независимых форм теории управления системами в единый формат [12]. Укрупненное схематичное представление полученного результата представлено на рисунке 1.

Принципиальное отличие данного представления обобщенной модели процессной обработки данных состоит в следующем:

- выявленные деструкторы по произвольной существующей классификации не представлены в форме возможных последствий, а также возможных форм защиты от негативных последствий. Комбинация деструктора и атакуемого информационного ресурса представляет пару исходных данных для узловой точки дерева событий. Цель – выявление возможных путей развития, построение сценария с альтернативными вариантами развития. Данная методология позволяет не анализировать деструктор не как отдельный элемент, а как часть самоорганизованной системы бот-сети;
- параллельно ведется анализ множества действующих деструкторов, а также конструкторов адаптивной защиты. Текущее состояние прописывается в фасет текущего состояние. Как было отмечено в предыдущих изданиях, особенностью фасета является граничность каждой ячейки. На текущий момент используются ячейки с шестью границами, в отличии от классической ячейки с четырьмя границами. За счет внесения искусственной избыточности удалось избежать коллизии при неопределенности решения;

– дискретное пространство баз ассоциаций позволяет упростить процесс обработки за счет упрощенной формы представления данных по аналогии трансформации битового представления при переходе от хранения в 8-битном формате в 6-битный для транспортировки по каналам связи. За счет того, что продукционные правила ограничены в символах, сформирован искусственный алфавит.

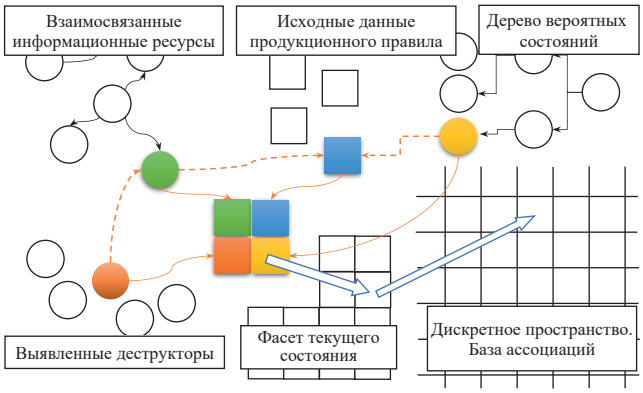

Рис. 1. Схема взаимодействия полуавтономной противоборствующей бот-сети интеллектуальных агентов и деструкторов цифровой инфраструктуры

Для формирования связей между двумя классами баз ассоциаций деструкторов и конструкторов используются оси идентификаторов матричного представления (рис. 2). Для визуального представления можно сформировать аффинную систему координат, где две плоскости – базы ассоциаций.

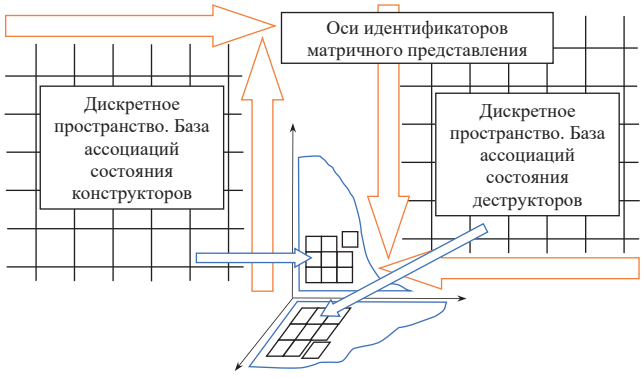

Рис. 2. Использование независимых фасетов организации данных баз ассоциаций интеллектуальных агентов бот-сети

Полученная кубическая матрица для связи двух граней состояний в форме дискретного пространства невзаимодействующих баз ассоциаций состояний конструктора / деструктора системы оснащается третьей составляющей – иерархия преобразования альтернативных состояний (рис. 3) [13].

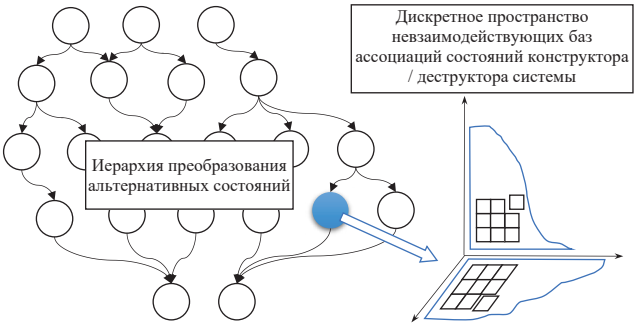

Рис. 3. Использование деревьев для формирования связей между состояниями интеллектуальных агентов бот-сети

Алгоритм формирования продукционного процессного правила бот-сети следующий:

– фасет деструкторов добавляет к каждому внедренному правилу координаты ячейки, определяет вероятных соседей по схожим признакам (первая часть решения);
– фасет конструкторов добавляет к каждому определенному правилу координаты ячейки, определяет схожие с деструктором по текущему состоянию признаки (вторая часть решения);
– производится поиск правила перехода к вероятному следующему состоянию в базе правил, строится узел дерева преобразования состояний (третья часть решения) (рис. 3).

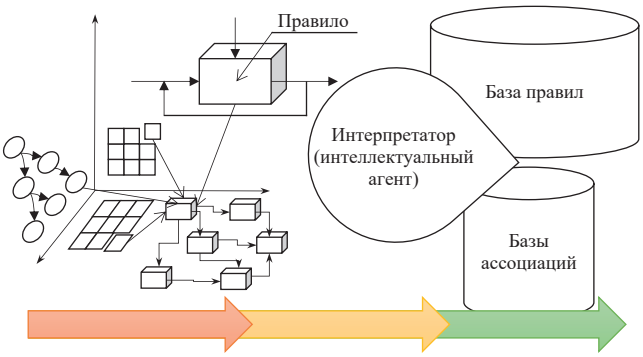

Рис. 4. Обобщенная схема интеграции противоборствующей бот-сети в единую цифровую среду

Как и в классическом представлении целевых иерархических деревьев, каждое алгебраическое правило снабжается индикатором состояния по принципу светофор. Данная методология используется в связи со своей простотой применения в рисковых моделях. Как следствие, каждый узел дерева снабжается рисковым двухкритериальным коэффициентом опасности в процентном соотношении и коэффициентом последствий в аналоге денежного эквивалента.

Заключение

Представленная методология использования разработанной модели широко описана во многих публикациях [14, 15], прошла апробацию в разных сферах профессиональной деятельности при формализации и дальнейшем применений результатов моделирования, а также в более 10 диссертационных исследований не только в пределах РФ. Успешное применение при составлении продукционных правил в упрощенной алгебраической форме теории мультимножеств на множестве процессов еще раз подтверждает тот факт, что отечественные разработки, совершенствующие семантическую составляющую теории информации, позволит перейти к более качественному уровню не только для защиты информации на уровне суверенного государства, но и для предупреждения возможных атак со стороны предполагаемых и уже действующих оппонентов[13].

13 Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситета

Литература

1. *Кевин Митник «Искусство обмана». – режим доступа: https://remarx.ru/media/books/ iskusstvo_obmana_mitnikpdf.pdf*
2. *Рыженко А. А. Умная бот-сеть или модель интеллектуального деструктора // Вопросы кибербезопасности. 2023. № 5(57). С. 60–68. DOI: 10.21681/2311-3456-2023-5-60-68*
3. *Gibert, D., Mateu, C., Planes, J. et al. Using convolutional neural networks for classification of malware represented as images. J Comput Virol Hack Tech 15, 15-28 (2019). https://doi.org/10.1007/s11416-018-0323-0*
4. *Bernardeschi, C., Domenici, A. & Palmieri, M. Formalization and co-simulation of attacks on cyber-physical systems. J Comput Virol Hack Tech 16, 63-77 (2020). https://doi.org/10.1007/s11416-019-00344-9*
5. *Jain, M., Andreopoulos, W. & Stamp, M. Convolutional neural networks and extreme learning machines for malware classification. J Comput Virol Hack Tech 16, 229-244 (2020). https://doi.org/10.1007/s11416-020-00354-y*
6. *Rahman, R.U., Tomar, D.S. Threats of price scraping on e-commerce websites: attack model and its detection using neural network. J Comput Virol Hack Tech 17, 75-89 (2021). https://doi.org/10.1007/s11416-020-00368-6*
7. *Reddy, V., Kolli, N. & Balakrishnan, N. Malware detection and classification using community detection and social network analysis. J Comput Virol Hack Tech 17, 333-346 (2021). https://doi.org/10.1007/s11416-021-00387-x*
8. *Ebrahim, M., Golpayegani, S. A. H. Anomaly detection in business processes logs using social network analysis. J Comput Virol Hack Tech 18, 127-139 (2022). https://doi.org/10.1007/s11416-021-00398-8*
9. *Рыженко А. А., Рыженко Н. Ю. Интеллектуальные деструкторы и мобильные банковские клиенты / Актуальные проблемы и перспективы развития экономики: Труды XXI Международной научно-практической конференции. Симферополь-Гурзуф, 20–22 октября 2022 год. / Под ред. д.э.н., д.пед.н., профессора Н. В. Апатовой. – Симферополь: Издательский дом КФУ им. В. И. Вернадского, 2022. – с. 241-242.*
10. *Рыженко А. А. Модифицированный алгоритм вируса полиморфика как основа деструктора информационной среды / Информатика: проблемы, методология, технологии: сборник материалов XVIII международной научно-методической конференции: в 7 т. / под редакцией Н. А. Тюкачева; Воронеж, Воронежский государственный университет, 14-15 февраля 2019 г. – Воронеж: Издательство «Научно-исследовательские публикации» (ООО «Вэлборн»), 2019. – Т. 5. – С. 857–861.*
11. *Рыженко А. А. Модель вложенной пирамиды системы управления безопасностью информационного пространства госкорпорации / Противодействие терроризму и экстремизму в информационных системах: сборник научных статей Всероссийской конференции – М.: Московский университет МВД России имени В. Я. Кикотя, 2020. – с. 65–69.*
12. *Рыженко А. А., Рыженко Н. Ю. Безопасность информации цифровой экономики / Актуальные проблемы и перспективы развития экономики. Труды Юбилейной XX Всероссийской с международным участием научно-практической конференции. Симферополь, 2021. С. 289–291.*
13. *Рыженко А. А. Фасетно-иерархическая модель как альтернатива существующим моделям систем поддержки управления / Управление информационными ресурсами. Материалы XIX Международной научно-практической конференции. Минск, 2023. С. 37-38*
14. *Любавский А. Ю. О необходимости развития алгоритмического мышления следователей в контексте расследования киберпреступлений / Проблемы противодействия киберпреступности. Материалы международной научно-практической конференции. Москва, 2023. – с. 105–108.*
15. *Любавский А. Ю. Актуальные вопросы обеспечения безопасности персональных данных в сети интернет / Обеспечение информационной безопасности: вопросы теории и практики. Сборник статей Всероссийской научно-практической конференции. Науч. редакторы Г. Г. Камалова, В. Г. Ившин, Г. А. Решетникова. Ижевск, 2023. – с. 39–45.*