Метод упреждения возмущений на киберсистемы Индустрии 4.0

С. А. Петренко
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
S.Petrenko@rambler.ru

Д. Е. Воробьева
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
DinVor@mail.ru

***Аннотация*. В настоящее время много усилий прилагается для создания методов и алгоритмов, которые могли бы обеспечить требуемую киберустойчивость киберсистем Индустрии 4.0. Широко распространено мнение, что средства обеспечения киберустойчивости должны обнаруживать и нейтрализовать деструктивные возмущения за минимальное время (секунды, минуты), для обеспечения резерва времени на восстановление цифровых платформ (от десятков минут до нескольких часов) и поддержания киберустойчивости на заданном уровне. Предложенный подход имеет право на существование, однако, наиболее приемлемым (желаемым) решением является такое, при котором деструктивные возмущения на цифровые платформы пресекаются до того момента, как будет осуществлен перевод в непоправимые катастрофические состояния. Последнее возможно только в том случае, если подсистема управления киберустойчивостью цифровых платформ будет обладать способностью заранее предупреждать о подобных воздействиях и их последствиях.**

Ключевые слова: Индустрия 4.0; цифровая экономика; киберустойчивость; интеллектуальная система управления киберустойчивостью; свойство предупреждения возмущений

I. Постановка задачи

В настоящее время наиболее пригодными системами для решения схожих задач являются системы обнаружения и предотвращения вторжений [1–10]. Здесь под системой обнаружения вторжений (СОВ) понимается программное и/или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления соответствующими сетевыми объектами. Как правило, СОВ используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной сети или системы. Например, для обнаружения сетевых атак против уязвимых сервисов, атак, направленных на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения.

Проведённый анализ возможностей средств обеспечения ИБ показал, что в настоящий момент наибольшее развитие получили средства, способные осуществлять распознавание известных атакующих воздействий, оповещение ответственных лиц о факте совершения атаки и её пресечение, и значительно меньше развиты средства, способные осуществлять накопление и интеллектуальную обработку данных, приводящую к возможности порождения спецификаций упреждающего поведения, составляющих основу формируемых экспертами решений по поддержанию безопасности КИИ. Для того чтобы система обеспечения информационной безопасности КИИ была способной предупреждать и пресекать информационно-технические воздействия на его элементы, она должна быть способной к ведению упреждающего противоборства и не может обойтись без подсистемы, способной осуществлять интеллектуальную обработку данных, поступающих на её вход. Именно в ходе интеллектуальной обработки данных интеллектуальная система (ИС) должна строить модели поведения противоборствующих сторон и только потом выбирать из построенных моделей модели упреждающего поведения в конфликте. Сформированные ИС модели должны быть представлены в виде соответствующих спецификаций либо эксперту (оператору), либо подсистеме управления средствами обеспечения ИБ. Естественно предположить, что детальность спецификаций при этом должна отличаться.

II. Предлагаемый подход

Рассмотрим процесс работы экспертов и интеллектуальной системы, представленной в виде системы поддержки принятия решений по предупреждению и противодействию компьютерным атакам, направленным на КИИ, как процесс *коммуникации риска*. Здесь вопрос, связанный с выработкой решений, способствующих не вовлечению в рискованную ситуацию или действий, предупреждающих вовлечение в неё, остаётся весьма актуальным (вопрос «предотвращения риска» – по ГОСТ Р ИСО/МЭК 27005-2010). Таким образом, цель взаимодействия экспертов с проектируемой системой в ходе предотвращения рисков должна сводиться к удовлетворению их информационных потребностей, связанных с получением от интеллектуальной системы, способной осуществлять порождение спецификаций упреждающего поведения в информационном конфликте (ИК), знаний (сведений), необходимых для управления

целями, задачами, рисками и проблемами в области обеспечения безопасности КИИ [3].

Само понятие <Предотвращение> предлагается декомпозировать в понятиях <Обнаружение>, <Предупреждение> и <Пресечение> (см. рис. 1). При этом, в рамках <Обнаружения> следует выделить <Узнавание> (распознавание) и <Открытие> (рассуждение с заключением), а в рамках <Предупреждения> – <Уведомление> (оповещение) и <Упреждение> (предварение) [3]. Способность автоматизированных систем поддержки принятия решений к противодействию, а точнее – к предотвращению КА на КИИ, должна основываться на способности к манипулированию имеющимися у системы знаниями и способности к порождению новых знаний (см. «Открытие» на рис. 1). Очевидно, что пополнять собственную базу знаний ИС может либо информацией, которая предоставляется ей экспертами и программными (аппаратно-программными) средствами из её состава, либо порождёнными ею знаниями, тем самым сокращая время пополнения базы знаний, а, следовательно, и время выработки решений по обеспечению защищённости КИИ.

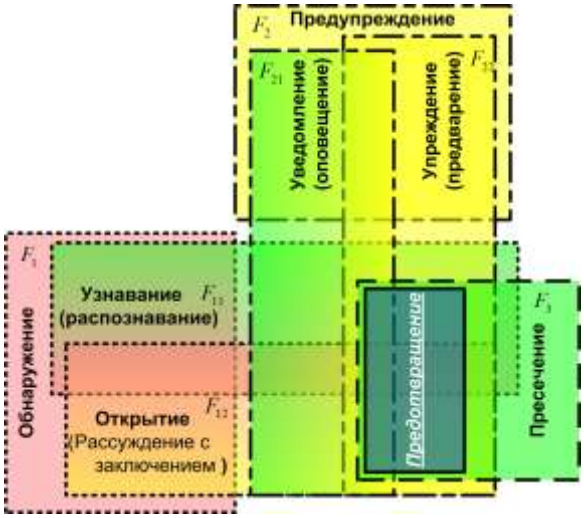

Рис. 1. Декомпозиция понятия <предотвращение>

Проектируемая система должна относиться к классу самоорганизующихся систем. Для этого необходимо, чтобы она была многоагентной, а сами программные, аппаратные и аппаратно-программные модули системы предотвращения компьютерных атак на КИИ имели потенциальную возможность унифицированного взаимодействия [2]. Для того чтобы проектируемая система была способна предотвращать новые виды воздействий (сценарии предотвращения которых не вносились непосредственно в систему при её создании), необходимо чтобы она была способна увеличивать мощность множества собственных потенциальных состояний (стратегий поведения) под воздействием внешних факторов [2]. Система порождения сценариев упреждающего поведения в конфликте является Интеллектуальной Системой. Интеллектуальные Системы [5, 6] (ИС) обладают специфической архитектурой, допускающей определенные вариации. Проектированием Интеллектуальных Систем, способных порождать (модифицировать) собственные модели поведения под влиянием внешних факторов, занимались и ранее в рамках исследований в области Искусственного Интеллекта (ИИ) в разделе Гироматов [7, 8], обоснованных Д.А. Поспеловым. Опираясь на идею Гиромата, а также на основы системно-организационного подхода в ИИ, включающие ряд принципов, выдвигается гипотеза о том, что самоорганизующаяся интеллектуальная система $\mathcal{K}$, способная к порождению спецификаций упреждающего поведения в конфликте, должна быть представлена в виде иерархии взаимодействующих Гироматов ($\mathcal{G}$). Упреждающее поведение системы $\mathcal{K}$ в конфликте сводится к синтезу такого сценария поведения, в ходе которого она способна изменить ход запланированного атакующей стороной процесса, приводящего к негативным последствиям. Для этого система $\mathcal{K}$ должна быть способной изменить ход одного из мероприятий, являющегося составной частью процесса, который может быть завершён с неприемлемым для защищаемых объектов (и/или $\mathcal{K}$) результатом. Изменение выполнения одного из мероприятий должно приводить к изменению процесса, а именно – к переходу к такой последовательности мероприятий (к траектории процесса), которая завершается допустимым для КИИ ($\mathcal{K}$) исходом.

Предлагается в АСППР реализовать метод интенсионального пополнения [15] онтологии [16], представленной в памяти гиромата $\mathcal{G}$, который основан на возможности вычисления значения функции в точке, находящейся вне области определения. В качестве значения функции в этой точке предлагается порождать новый синтаксический объект, отражающий факт вызова в ней. Этот объект определяется как строка, полностью совпадающая с текстом вызова. Такой способ доопределения функций называется задержкой функции. Использование задержки функций позволяет задать абстракцию предвычислений. Значение, получающееся в результате такой задержки, называют *интенсионалом*. Оба указанных метода порождения новых знаний должны быть реализованы в $\mathcal{G}$ и должны выполняться во взаимосвязи друг с другом, что позволит $\mathcal{G}$ не только дополнять онтологию достроенными Ролями, но и встраивать в упорядоченное множество Концептов новые Концепты, порождённые в ходе интенсионального расширения, что значительно расширит способности $\mathcal{G}$, связанные с анализом и описанием многоэтапных взаимодействий различных объектов и субъектов (рис. 2).

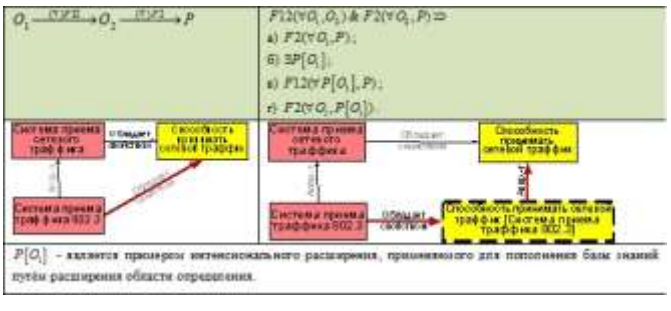

Рис. 2. Пример осуществления интенсионального расширения, применяемого для исполнения базы знаний путём расширения области определения

Однако порождения новых знаний указанными методами недостаточно для синтеза спецификаций процессов, описывающих стратегии упреждающего поведения в конфликте и предотвращения воздействий на КИИ. В ходе синтеза указанных спецификаций предлагается дополнительно использовать метод установления семантического подобия моделей <Задач> и <Решений> по аналогии.

Ядро метода установления семантического подобия моделей <Задач> и <Решений> по аналогии основано на возможности $\mathcal{G}$ в общем случае осуществлять переход от аппроксимирующих Концептов (а, следовательно, и процессов), принадлежащих одной ПрО (или одному объекту защиты), через аппроксимируемые (более общие) к аппроксимирующим, но принадлежащим другой ПрО (другому типовому объекту защиты) [11].

Ввиду того, что в результате поиска <Задач> и <Решений> по аналогии может быть порождено множество спецификаций, так как в ряде случаев «спуск» по частично упорядоченному множеству Концептов (от аппроксимируемых к аппроксимирующим) может приводить к помещению в ФВ целого ряда Концептов, находящихся на одном уровне в частично упорядоченном множестве (т.е. несравнимых между собой), предлагается использовать возможности аппарата аппликативно-комбинаторных вычислений, что способствует реализации в $\mathcal{G}$ процедуры направленного комбинирования, основанной на применении ограниченного перечня доступных функциональных форм ($\left[\left[O_1 \to P_1\right] \to A_1\right] \to \left[O_2 \to P_2\right]$, что означает: «Объект O_1, обладающий свойством P_1, способен осуществить воздействие A_1 на объект O_2, поскольку последний обладает свойством P_2»), что позволит уменьшить число порождаемых некорректных спецификаций ещё на этапе их формирования. Т.е., решение о потенциальной «реализуемости» («нереализуемости») процесса, описываемого формируемой спецификацией, $\mathcal{G}$ может принимать на основе знаний, извлечённых из построенной онтологии, так как в ней имеются данные о типах объектов (в виде решётки Концептов) и функциональных типах (в виде решётки Ролей), а данная информация даст возможность $\mathcal{G}$ правильно сочетать имеющиеся у него комбинаторы (в качестве функций) и данные (в качестве аргументов).

В общем случае результатом комплексного применения указанных методов являются порождённые Гироматом спецификации, пригодные для организации процессов по предотвращению возможных атакующих воздействий. Очевидно, что детализация спецификаций может быть различной, вплоть до конкретных программ по управлению конкретными агентами сенсорами и эффекторами.

III. Заключение

Очевидно, что решение задач упреждения компьютерных атак на КИИ опирается на результаты решения задач, связанных с обнаружением атакующих воздействий, которые в ближайшей или отдалённой перспективе могут привести к негативным последствиям для элементов КИИ и КИИ в целом. Ввиду этого, необходимо иметь возможность раннего обнаружения таких атакующих воздействий, по итогам наблюдений. Наблюдаемый $\mathcal{K}$ комплекс мероприятий потенциально может иметь различный состав включаемых мероприятий и связей между ними, а, следовательно, он обладает переменной структурой. Каждый возможный состав мероприятий, включённый в комплекс, а также связи между ними характеризуют конкретный вариант структуры комплекса, а точнее – конкретную возможную реализацию того или иного наблюдаемого процесса. Множество таких вариантов, известных $\mathcal{G}$ и представленных в его памяти в виде фрагментов онтологии, не более чем счётно, а следовательно процедура поиска и извлечения спецификаций процессов из памяти $\mathcal{G}$ конечна, а если учесть возможности, предоставляемые механизмом распространения АС по АРС, то и эффективно направлена.

Учитывая параметры АРС, однозначно связанной с онтологией, в которой представлены различные варианты структуры комплекса, можно считать, что $\mathcal{G}$ в своей памяти содержит комплексы мероприятий с вероятностной структурой. Для каждого варианта структуры комплекса мероприятий с вероятностной структурой можно построить свою сетевую модель (сеть). Так как при этом любой вариант имеет детерминированную структуру, то сетевые модели вариантов комплекса с вероятностной структурой будут сетями с детерминированной структурой, которые и представляют собой конкретные спецификации обнаруженных (сформированных) процессов. Для того, чтобы в рамках метода пресечения деструктивных воздействий в гетерогенной сетевой инфраструктуре с использованием интеллектуальных МАС стало возможным осуществить выбор такой стратегии поведения $\mathcal{K}$, которая привела бы к приемлемому выходу из конфликтной ситуации, развивающейся в рамках информационно-технического противоборства, необходимо, чтобы мероприятия моделируемого процесса, представленные в онтологии, сопровождались временными параметрами, характеризующими длительности их выполнения.

Таким образом, можно сделать вывод, что информационно-технические системы, способные синтезировать сценарии упреждающего поведения систем кибербезопасности в ходе ИК, должны найти широкое применение в области обеспечения информационной безопасности, что в свою очередь должно способствовать повышению уровня защищенности критических информационных инфраструктур при осуществлении на них компьютерных атак.

Список литературы

[1] Климов С.М. Методы и модели противодействия компьютерным атакам / С.М.Климов. Люберцы.: КАТАЛИТ, 2008. 316 с.

[2] Бирюков Д.Н., Ломако А.Г., Ростовцев Ю.Г. Облик антиципирующих систем предотвращения рисков реализации киберугроз // Труды СПИИРАН. 2015. № 2(39). С. 5–25.

[3] Бирюков Д.Н., Ломако А.Г. Подход к построению систем информационной безопасности, способных синтезировать сценарии упреждающего поведения в информационном конфликте // Защит информации. INSIDE. 2014.№ 6. С. 42-50.

[4] Финн В.К. Об интеллектуальном анализе данных // Новости Искусственного интеллекта. 2004. № 3. С. 3–18.

[5] Финн В.К. Искусственный интеллект: Идейная база и основной продукт // Труды 9-ой национальной конференции по искусственному интеллекту. М.: Физмат-лит. 2004. Т. 1. С. 11–20.

[6] Бирюков Д.Н. Подход к построению непротиворечивой теории синтеза сценариев упреждающего поведения в конфликте / Д.Н. Бирюков, Ю.Г. Ростовцев // Труды СПИИРАН. 2015. №1(38). С. 94-111.

[7] Бирюков Д.Н., Ломако А.Г. Формализация семантики для представления знаний о поведении конфликтующих сторон // Материалы 22-й научно-практической конференции «Методы и технические средства обеспечения безопасности информации». СПб.: Изд-во Политехн. ун-та. 2013. С. 8-11.

[8] Бирюков Д.Н. Абдуктивный синтез структур функциональных типов сценариев для установления аналогий в многомодельной концептуально-онтологической системе знаний / Д.Н. Бирюков, А.Г. Ломако, Т.Р. Сабиров // Труды СПИИРАН. 2017. № 4(53). С. 140-159.

[9] Бирюков Д.Н. Денотационная семантика контекстов знаний при онтологическом моделировании предметных областей конфликта / Д.Н. Бирюков, А.Г. Ломако // Труды СПИИРАН. 2015. № 5(42). С. 155-179.

[10] Бирюков Д.Н., Ломако А.Г., Сабиров Т.Р. Многоуровневое моделирование сценариев упреждающего поведения // Проблемы информационной безопасности. Компьютерные системы. С-Пб.: Изд-во Политехнического университета. 2014. №4. С. 41-50.

[11] Бирюков Д.Н. Модель изменения доступности знаний, представленных в памяти киберсистемы, обеспечивающей нейтрализацию деструктивных воздействий на объекты критической информационной инфраструктуры / Д.Н. Бирюков, Т.Р. Сабиров, С.В. Пилькевич, А.П. Глухов // Журнал «Наукоемкие технологии в космических исследованиях Земли». 2016. Т.8. № 4 С. 56-63.

[12] Бирюков Д.Н. Пополнение онтологических систем знаний на основе моделирования умозаключений с учетом семантики ролей / Д.Н. Бирюков, А.Г. Ломако, Р.Б. Жолус // Труды СПИИРАН. 2016. № 4(47). С. 105-129.

[13] Зотова А.В., Ломако А.Г., Петренко С.А. Система администрирования устойчивости и безопасности вычислений. В сборнике: Дистанционные образовательные технологии. Материалы III Всероссийской научно-практической конференции. Ответственный редактор В.Н. Таран. 2018. С. 346-353.

[14] Ломако А.Г., Овчаров В.А., Петренко С.А. Метод расследования инцидентов безопасности на основе профилей поведения сетевых объектов. В сборнике: Дистанционные образовательные технологии. Материалы III Всероссийской научно-практической конференции. Ответственный редактор В.Н. Таран. 2018. С. 366-373.

[15] Маковейчук К.А., Петренко А.С., Петренко С.А. Метод контроля корректности технологических платформ цифровой экономики на основе разделения компонент. В сборнике: Информационные системы и технологии в моделировании и управлении. Сборник материалов III Всероссийской научно-практической конференции с международным участием, посвященной 100-летию Крымского федерального университета имени В.И. Вернадского. Ответственный редактор К.А. Маковейчук. 2018. С. 260-263.

[16] Маковейчук К.А., Петренко А.С., Петренко С.А. Методика оптимизации матриц размерности технологических платформ цифровой экономики. В сборнике: Информационные системы и технологии в моделировании и управлении. Сборник материалов III Всероссийской научно-практической конференции с международным участием, посвященной 100-летию Крымского федерального университета имени В.И. Вернадского. Ответственный редактор К.А. Маковейчук. 2018. С. 264-270.

[17] Шмелев В.В., Ломако А.Г., Петренко С.А. Трансформационный синтез функционально-логических схем программ в вычислительных сетях Петри с верификацией корректности свойств вычислимости. В сборнике: The 2018 Symposium on Cybersecurity of the Digital Economy (CDE18). [Вторая международная научно-техническая конференция]. Санкт-Петербург, 2018. С. 316-338.