УДК 004.8:007.3

Д.Н. Бирюков, А.Г. Ломако, Ю.Г. Ростовцев

ОБЛИК АНТИЦИПИРУЮЩИХ СИСТЕМ ПРЕДОТВРАЩЕНИЯ РИСКОВ РЕАЛИЗАЦИИ КИБЕРУГРОЗ

Бирюков Д.Н., Ломако А.Г., Ростовцев Ю.Г. **Облик антиципирующих систем предотвращения рисков реализации киберугроз.**
Аннотация. Предлагается облик интеллектуальных систем кибербезопасности со свойством антиципации. Обосновывается необходимость того, что система предотвращения компьютерных атак должна быть представлена в виде самообучающейся интеллектуальной системы самоорганизующихся гироматов. Ожидается, что применение искомых систем на практике, должно позволить более успешно решать задачи, связанные с предотвращением рисков реализации киберугроз.
Ключевые слова: антиципация, гиромат, киберсистема, предотвращение, семантика.

Biryukov D.N., Lomako A.G, Rostovtsev Y.G. **The Appearance of Anticipating Cyber Threats Risk Prevention Systems.**
Abstract. The appearance of intelligent cybersecurity systems featuring the property of anticipation is proposed. It is substantiated that the system of cyber attacks prevention should be designed in the form of self-learning intellectual self-organizing Gyromats system. It is expected that the application of the sought-for systems in practice would allow to solve problems related to prevention of cyber threats more efficiently.
Keywords: anticipation, gyromat, cybersystem, prevent, semantics

1. Введение. В настоящее время вопросам обеспечения информационной безопасности (ИБ) посвящается большое количество работ как у нас в стране, так и за рубежом. Но несмотря на это, ситуация складывается таким образом, что на сегодняшний день в арсенале средств обеспечения ИБ превалируют средства нейтрализации компьютерных атак (КА) на заключительных этапах их проявления, и практически отсутствуют механизмы, позволяющие осуществлять их упреждающее пресечение. Таким образом, на современном этапе развития средств обеспечения ИБ назрела объективная необходимость создания новых систем, способных осуществлять предотвращение возможных КА на защищаемые ресурсы [1]. Наиболее близкими по функционалу к искомым системам, являются системы предотвращения вторжений (СПВ). Однако, как показывает практика применения СПВ, они способны детектировать и частично отражать уже осуществляющиеся воздействия, но не в состоянии заблаговременно пресечь атакующие воздействия. Не способна к этому и вся совокупность существующих средств без соответствующей доработки и серьезного вмешательства квалифицированного специалиста в процесс их взаимного функционирования. Тем не менее вопрос, связанный с выработкой

решений, способствующих не вовлечению в рискованную ситуацию, или действий, предупреждающих вовлечение в нее, остается весьма актуальным (вопрос "предотвращения риска"). Следовательно актуальным является и вопрос создания системы, способной строить спецификации процессов упреждающего поведения в информационно-техническом конфликте.

2. Предотвращение – генеральная цель обеспечения ИБ. Можно утверждать, что цель взаимодействия экспертов с проектируемой системой в ходе предотвращения рисков должна сводиться к удовлетворению их информационных потребностей, связанных с получением от интеллектуальной системы (ИС), способной осуществлять порождение спецификаций упреждающего поведения в конфликте, знаний (сведений), необходимых для управления целями, задачами, рисками и проблемами в области обеспечения ИБ защищаемой организации. Чем большим количеством специальных знаний (адаптированных, содержащих модели возможных решений) обладает ИС, тем более полезна она может быть для экспертов в их деятельности, связанной с предотвращением риска.

Понятие «предотвращение» не является тривиальным. Как показывает анализ публикаций, не всегда понятие «предотвращение» истолковывается одинаково даже учеными единомышленниками. Ввиду этого видится необходимым декомпозировать рассматриваемое понятие на осмысленные составляющие.

Как видится, понятие «Предотвращение» (устранение ранними мерами) является агрегирующим понятием и основывается на понятиях «Обнаружение», «Предупреждение» и «Пресечение». При этом в рамках «Обнаружения» можно выделить «Узнавание» (распознавание) и «Открытие» (рассуждение с заключением), а в рамках «Предупреждения» – «Уведомление» (оповещение) и «Упреждение» (предварение).

Анализ возможностей средств обеспечения ИБ позволяет сделать вывод о том, что в настоящий момент наибольшее развитие получили средства, способные осуществлять распознавание известных атакующих воздействий (КА), оповещение должностных лиц о факте их совершения и пресечение КА. Значительно меньше развиты средства, способные осуществлять накопление и интеллектуальную обработку данных, приводящую к возможности порождения спецификаций упреждающего поведения.

Можно предположить, что способность системы обеспечения ИБ к упреждению в конфликте основывается на способности к манипулированию имеющимися у системы знаниями и способности к по-

рождению новых знаний (см. «Открытие»). Очевидно, что пополнять собственную базу знаний (БЗ) система обеспечения ИБ конкретной критической информационной инфраструктуры (КИИ) может либо информацией, которая предоставляется ей экспертами и программными (аппаратно-программными) средствами из ее состава, либо порожденными ею знаниями, тем самым сокращая время пополнения базы знаний, а следовательно и время выработки решений по обеспечению защищенности КИИ.

Пусть, например, к моменту времени t_0 система предотвращения КА накопила данные, необходимые и достаточные для построения моделей, возможно реализуемых в ходе информационно-технического конфликта (ИТК) процессов, схематично представленных в виде различных траекторий на рисунке 1. При этом различные процессы могут быть потенциально завершены с различными результатами. Некоторые результаты приемлемы для КИИ, а некоторые нет (см. оценки от «-3» до «+2»). Важным моментом является то, что система обеспечения ИБ КИИ может на отдельных этапах потенциально реализуемых процессов повлиять на их ход (см. узлы «B», «D», «E», «F», «I»). Очевидно, что чем быстрее система обеспечения ИБ КИИ смоделирует возможно реализуемые процессы, тем больше альтернатив упреждающего поведения она сможет предложить оператору.

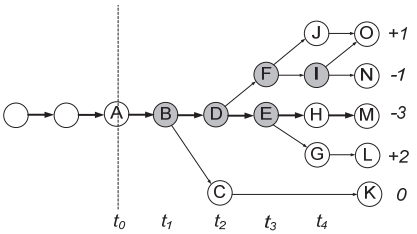

Рис. 1. Траектории возможно реализуемых в ходе ИТК процессов

Пусть наиболее вероятен процесс «A-M», который завершается с наихудшим исходом («-3»). Тогда, если системе обеспечения ИБ КИИ для моделирования процессов ИТК и выбора приемлемого варианта упреждающего поведения требуется $t_3 - t_0$ времени, то она не сможет предложить оператору ни одного приемлемого решения, если же системе потребуется менее чем $t_1 - t_0$ времени, то она сможет предложить целый ряд альтернатив. Таким образом, можно предположить, что чем более интеллектуальна система, тем в большем количестве и более скоро она способна выработать спецификации упреждающего поведения в ходе ИТК.

Следовательно, можно утверждать, что упреждающее поведение киберсистемы в конфликте сводится к синтезу такого сценария поведения, в ходе которого она способна изменить ход запланированного к реализации противником процесса, приводящего к негативным для КИИ последствиям. Для этого киберсистема должна быть способной изменить ход одного из мероприятий, являющегося составной частью процесса, который может быть завершен с неприемлемым для КИИ (киберсистемы) результатом. Изменение выполнения одного из мероприятий должно приводить к изменению процесса, а именно – к переходу к такой последовательности мероприятий (к траектории/трассе процесса), которая завершается допустимым для КИИ (киберсистемы) исходом.

Ввиду этого проблему исследования вопросов обеспечения защищенности КИИ в ходе ИТК предлагается свести к построению системы порождения сценариев упреждающего поведения в конфликте. Как видится, именно системы порождения сценариев упреждающего поведения в конфликте должны стать основой систем предотвращения компьютерных атак. При этом они не позиционируются как альтернатива существующим системам, обеспечивающим ИБ КИИ, а призваны лишь дополнить ее.

3. Антиципация – ключевой механизм упреждения в конфликте. На начальном этапе при поиске подходов к реализации в искомой системе упреждающего поведения предлагается обратить внимание на поведение биосистем, так как именно живые организмы и биосистемы выживают и эволюционируют уже много десятков миллионов лет, а поэтому видится целесообразным перенять часть опыта у них и заложить его в проектируемую систему обеспечения ИБ КИИ.

Проведенный анализ поведения живых существ и биосистем [2] позволил выявить ряд типовых механизмов их поведения, результатом которого является предотвращение возможных негативных для них последствий. Ряд механизмов упреждающего поведения изначально “вшит” в биоорганизмы. Это – рефлексы, иммунная система и другие. Однако наиболее целесообразному результативному упреждающему поведению животные и человек обучаются в ходе своей жизни, передавая и развивая его в поколениях. Очевидно, что одно из ведущих мест в процессе обучения в целом и в процессе разработки стратегий упреждающего поведения – в частности, играет головной мозг и механизмы мышления, реализованные в нем. Одним из примечательных механизмов является «*антиципация*». Так, например, Б.Ф.Ломов понимает антиципацию как «способность (в самом широком смысле) действовать и принимать те или иные решения с определенным вре-

менно-пространственным упреждением в отношении ожидаемых, будущих событий». Очевидно, что понятие антиципации может быть с пользой применимо не только к психической деятельности человека, но и к деятельности систем обеспечения информационной безопасности [3].

Можно предположить, что для того чтобы киберсистема обеспечения ИБ могла обладать свойством антиципации, она должна быть способной (см. рисунок 2): получать информацию через систему сенсоров (1.1, 1.2); оперировать информацией о прошлом опыте системы (2.1, 2.2); сопоставлять полученную информацию с имеющейся (3.1, 3.2); выдвигать гипотезы о возможных в перспективе событиях (4.1, 4.2); порождать стратегии целенаправленного поведения системы (5.1, 5.2); поддерживать требуемый уровень защищенности КИИ (6.1, 6.2).

Рис.2. Принципиальная схема антиципирующей системы

Интеллектуальную систему со свойством антиципации, способную осуществлять предотвращение атакующих воздействий на защищаемую КИИ, на начальном этапе практически невозможно описать полно и детально. Поэтому функционирование проектируемой системы предлагается рассмотреть через многомодельное представление процессов взаимодействия конфликтующих сторон и описать на нескольких стратах, приведенных в работе [1]. Понимание системы возрастает при последовательном переходе от одной страты к другой: чем ниже осуществляется спуск по иерархии, тем более детальным становится раскрытие системы, чем выше подъем, тем яснее становится смысл и значение всей системы.

Верхняя страта (искомая способность киберсистемы): предотвращение негативных компьютерных атак на защищаемую КИИ.

Нижняя страта (киберинтерпретация антиципации):

– сбор данных от сенсоров (рецепторов): распознавание элементарных явлений, регистрируемых специальными программными модулями, распределенными в сетевой инфраструктуре;

– классификация наблюдаемых элементарных явлений (агрегирование собираемых данных о наблюдаемых явлениях до уровня элементарных событий; формирование информационных признаков, присущих возможным опасностям);

– выявление типов потенциально возможных опасностей путем построения моделей потенциально реализуемых атакующей стороной процессов;

– определение существования задачи (задачи, требующей обращения на нее внимания) среди тех потенциальных опасностей, которые могут исходить от атакующей стороны;

– синтез схем потенциально возможного поведения системы предотвращения компьютерных атак (определение типовых решений, которые уже были выработаны системой предотвращения атакующих воздействий на более ранних этапах ее функционирования, либо были заложены в нее разработчиками; определение схем потенциально реализуемых вариантов решений, осуществляемое в случае отсутствия типовых решений);

– выбор конкретного варианта поведения из существующих (построенных): выбор наиболее подходящего варианта поведения для разрешения идентифицированного конфликта;

– построение стратегии реализации выбранного решения, направленного на упреждение потенциальных опасностей, на уровне операций;

– конструирование схем нейтрализации возможных угроз (конструирование схемы нейтрализации угроз на уровне операторов; формирование схемы управления системой сенсоров и эффекторов на уровне микроопераций, с целью пресечения компьютерных атак);

– верификация схемы управления эффекторами (и/или сенсорами).

Проведенный анализ показал, что как правило КИИ представляет собой разнородную (гетерогенную) распределенную сетевую инфраструктуру, а ее элементы потенциально уязвимы [3]. При этом уязвимости могут содержать различные как по назначению, так и по способу реализации элементы КИИ. Несмотря на это, проектируемая киберсистема предотвращения возможных атакующих воздействий (компьютерных атак) на КИИ ($\mathcal{K}$) должна быть потенциально способной функционировать в указанных условиях и учитывать дан-

ные факты при порождении сценариев упреждающего поведения в конфликте.

4. Самоорганизация – необходимое свойство системы, способной порождать сценарии упреждающего поведения в конфликте. Термин «самоорганизующаяся система» ввел У.Р. Эшби еще в середине прошлого века, но, к сожалению, до сих пор неизвестны достаточные условия, выполнение которых гарантировало бы начало самоорганизации. Сам же У.Эшби выделил два различных значения термина «самоорганизующаяся система» [4].

Во-первых, самоорганизация может заключаться в переходе «от системы с независимыми частями к системе с зависящими друг от друга частями» [4], при этом не учитывается, хороша или плоха возникающая организация. Системы такого рода Эшби предложил называть «самосвязующимися» (далее – «Самоорганизация_I»).

Во-вторых, самоорганизацией можно считать переход от плохой организации к хорошей, когда, например, ребенок, вначале потянувшись к огню, затем уже избегает его [4] (далее – Самоорганизация_II"). Правда, оговаривается Эшби: «…не существует «хорошей организации» в абсолютном смысле. Она всегда относительна...» [4].

Когда рассматривается Самоорганизация_II, то особенно важным является то, что самоорганизующаяся система сама переходит от "плохого" поведения к "хорошему".

Пусть множество состояний системы – S, а f – отображение S в S и определяется как множество пар (s_i, s_j), таких, что внутренняя движущая сила системы будет переводить состояние s_i в s_j. Если f является только функцией состояния (т.е. она может быть точно определена), то систему нельзя назвать "самоорганизующейся" [4].

Тогда, пусть функция f изменяема, а сами изменения не могут быть приписаны какой-либо причине во множестве S, то такой причиной может быть только некоторый внешний агент, воздействующий на систему S как ее вход. Если система должна быть в каком-то смысле "самоорганизующейся", понятие "само" должно быть расширено так, чтобы включать переменную α, причем для того, чтобы целое было ограничено, необходимо, чтобы причина изменений α находилась в S (или α). Таким образом, "самоорганизующейся" может быть только та система S, которая соединена с другой системой (из одной части). Тогда часть S может быть названа "самоорганизующейся" внутри целого $S+\alpha$. Только в этом частном и строго определенном

смысле можно признать, что система является “самоорганизующейся”, не будучи одновременно “самопротиворечивой” [4].

Утверждение 1. Необходимо, чтобы система $\mathcal{K}$ относилась к классу *самоорганизующихся систем*.

Доказательство:

“Самоорганизация_I”.

Лемма 1.1. Система $\mathcal{K}$ должна быть многоагентной

Доказательство.

КИИ представляет собой разнородную распределенную сетевую инфраструктуру [3], а ее элементы потенциально уязвимы, соответственно, необходимость наличия многоагентной системы предотвращения атакующих воздействий (КА) можно доказать следующим образом:

– пусть $OBG = \{obj_1, obj_2\}$ - множество взаимодействующих уязвимых элементов КИИ, причем obj_2 - целевой объект атаки;

– пусть $ACT = \{act_1, act_2, act_3\}$ - множество атакующих воздействий;

– $act_1(obj_1) = obj_1'$ - состояние элемента obj_1 КИИ после осуществления недопустимого воздействия act_1;

– пусть $act_2(act_1(obj_1), obj_2) = act_2(obj_1', obj_2) = obj_2'$ – двухэтапная атака;

– $act_2(obj_1, obj_2) = obj_2$ - выполнение второго этапа двухэтапной атаки при неуспешном выполнении первого этапа;

– $act_3(obj_1, obj_2) = act_3(obj_1', obj_2) = obj_2'$, где obj_2' - состояния элемента obj_2 КИИ после осуществления недопустимого воздействия act_3;

– пусть $IIPS = \{iips_a, iips_b, iips_c ...\}$ - элементы системы $\mathcal{K}$;

– пусть $P\_OBG = \{obj_1, obj_2, obj_3 ...\}$ - множество защищаемых ресурсов.

Допустим, система $\mathcal{K}$ может состоять из одного элемента:

– пусть $IIPS = \{iips_a\}$, т.е. $|IIPS| = 1$, а средство $iips_a$ - способно пресечь act_1;

– пусть $P\_OBG = \{obj_1\}$;

– тогда $iips_a\left(act_1\left(obj_1\right)\right) = obj_1$ означает, что $iips_a$ контролирует функционирование obj_1 и способно нейтрализовать атакующее воздействие $act_1\left(obj_1\right)$ в ходе его реализации. Очевидно, что и $act_2\left(iips_a\left(act_1\left(obj_1\right)\right), obj_2\right) = act_2\left(obj_1, obj_2\right) = obj_2$, однако act_3 способно воздействовать на obj_2 из состава КИИ (см. $OBG = \left\{obj_1, obj_2\right\}$ и $P\_OBG = \left\{obj_1\right\}$): $act_3\left(obj_1, obj_2\right) = obj_2'$, что является недопустимым. Следовательно, система предотвращения атакующих воздействий (КА) на КИИ в общем случае не может быть представлена системой, состоящей из одного элемента.

△ *Лемма 1.1.*

Лемма 1.2. Агенты системы $\mathcal{K}$ должны иметь возможность взаимодействовать друг с другом.

Доказательство.

Доказательство может быть выстроено на основе положений из двух ниже приведенных аксиом, сформулированных по результатам анализа порядка осуществления и пресечения атакующих воздействий.

Аксиома 1.2.1. Подавляющее большинство информационно-технических воздействий относится к классу многоэтапных.

Аксиома 1.2.2. Существуют мероприятия, связанные с предотвращением (пресечением) многоэтапных атакующих воздействий, при проведении которых результативность последующих этапов их выполнения зависит от результативности выполнения предыдущих этапов.

△ *Лемма 1.2.*

Простейший пример – киберсистема, состоящая из совокупности агентов сенсоров, измеряющих определенные параметры процессов, протекающих в киберпространстве, и агентов эффекторов, прерывающих определенные процессы из обнаруженных (на основании результатов измерений).

“Самоорганизация_II”.

Лемма 1.3. Система $\mathcal{K}$ для предотвращения новых видов воздействий должна быть способна порождать результативные стратегии поведения под влиянием внешней среды

Доказательство:

Для формулирования доказательства полезно ввести ряд обозначений, формализующих некоторые процессы, описывающие поря-

док функционирования киберсистемы с упреждающим поведением, реализуемым на основе антиципации:

– обнаружение воздействия ($act_i \in ACT$) производится через осуществление определенных измерений сенсорами системы: поступающие на вход(ы) системы в конкретный момент времени (T) данные (X), преобразовываются в данные (X_S), регистрируемые системой – $S: X \times T \to X_S$; S можно считать отображением, отвечающим за измерения;

– $Pr: D \times X_S \to L_{SM}$ – отображение регистрируемых данных (X_S) в формализованный вид представления (L_{SM}) для их последующего хранения и обработки (D задает порядок трансляции X_S в L_{SM});

– $M: L_{SM} \times Z_M \to Z_M$ – изменение (добавление) моделей (спецификаций, программ), которыми располагает система (изменение осуществляется под воздействием входных данных;

– $F: L_{SM} \times Z_M \to Z_{MeS}$, выбор стратегии поведения системы исходя из зарегистрированных данных и состояния системы (Z_{Mes} – модель действий системы);

– поскольку киберсистема должна быть способной не только принимать, но и передавать данные (а также осуществлять и другие активные действия), то необходимо реализовать отображение данных, хранящихся в системе в конкретный момент времени (T) и входящих в модель $Z_{Mes} \in Z_M$, в данные, формируемые на выходе системы (Y) – $R: D \times Z_{MeS} \times T \to Y$, где $D \times Z_{MeS} \to Y_S$.

Исходя из введенных выше обозначений, можно утверждать, что выбор стратегии поведения системой $\mathcal{K}$ в общем случае зависит от данных, поступающих из сторонней системы (систем) – см зависимость Z_{Mes} от X:

$$Z_{MeS} = F\left(L_{SM}, Z_M\right) = F\left(L_{SM}, M\left(L_{SM}, Z_M\right)\right) =$$
$$= F\left(Pr\left(D, X_S\right), M\left(Pr\left(D, X_S\right), Z_M\right)\right) =$$
$$= F\left(Pr\left(D, S\left(X, T\right)\right), M\left(Pr\left(D, S\left(X, T\right)\right), Z_M\right)\right).$$

△ *Лемма 1.3.*

Примечание: на формирование и выбор стратегии поведения системой предотвращения атакующих воздействий (КА) на КИИ также оказывают непосредственное влияние способности системы, связанные с преобразованием, накоплением и обработкой входных данных

во взаимосвязи с уже имеющейся информацией (с имеющимися моделями) – см. доказательство *Леммы 1.3*. Указанные способности реализуемы только в интеллектуальных системах.

▲ *Утверждение 1.*

5. Система порождения сценариев упреждающего поведения в конфликте – Интеллектуальная Система. Вопрос, связанный с тем, какую систему можно считать Интеллектуальной, остается открытым до сих пор. Ввиду этого, предлагается под Интеллектуальной Системой понимать такую систему, которая соответствует положениям, сформулированным В.К Финном [5, 6].

Интеллектуальные системы обладают специфической архитектурой, допускающей определенные вариации. Схематически эта архитектура может быть представлена следующим образом [5]:

ИС = (1) Решатель задач + (2) Информационная среда + (3) Интеллектуальный интерфейс.

(1) Решатель задач = (1.1) Рассуждатель + (1.2) Вычислитель + (1.3) Синтезатор.

(1.1) Рассуждатель реализует синтез и взаимодействие познавательных процедур, образующих автоматизированное рассуждение, областью применимости которого является класс задач, решаемых посредством формализованной эвристики. Логическим средством формализации этой эвристики и являются рассуждения. Правдоподобные рассуждения являются основным инструментом *Решателя* ИС реализуемым в *Рассуждателе* [6].

Существуют два типа *Рассуждателей*. *Рассуждатели первого типа* применимы к неизменяющемуся множеству исходных высказываний, характеризующих «замкнутый мир», а *Рассуждатели второго типа* реализуют формализованные эвристики для решения классов задач, исходными данными которых являются изменяемые и пополняемые множества высказываний (под изменением высказываний понимается пересмотр его истинностного значения, соответствующие базы фактов называют эпистемическими). *Рассуждатели второго типа* применимы к «открытым мирам», а их рассуждения называют когнитивными (правдоподобными) рассуждениями [5].

(1.2) Вычислитель применяется к числовым данным, используя численные методы, релевантные целям ИС.

(1.3) Синтезатор выбирает стратегии, адекватные не только цели ИС, но и состоянию БФ, и результатам предыдущих применений Решателя.

Если через Γ обозначить множество правил вывода, содержащих как правила достоверного вывода, так и правила правдоподобных

выводов, а через C – множество вычислительных процедур, то их комбинирование осуществляет *Синтезатор*.

(2) Информационная среда = (2.1) база фактов (БФ)+(2.2) база знаний (БЗ).

(2.1) БФ представляет рассматриваемую предметную область («замкнутый мир» или «открытый мир»; в первом случае БФ не изменяется, во втором – возможно ее пополнение в соответствии с результатами, полученными *Решателем* задач, и желаниями пользователя ИС как человеко-машинной системы).

Каждое элементарное событие – это элемент некоторого отношения. Фрагмент же предметной области характеризуется заданной системой отношений $R_1^{(k_1)},...,R_s^{(k_s)}$, с арностью $k_1,...,k_s$, соответственно.

Факт есть элементарное высказывание p_{ij} языка представления знаний L с некоторой оценкой v_{ij}, представляющее j-ый элемент отношения $R_i^{(k_i)}$, где $i = 1,...,s$. Таким образом, БФ есть множество элементарных высказываний p_{ij} с оценкой v_{ij}.

Наличие БФ как подсистемы ИС создает возможность осуществления машинного обучения [7], а, следовательно, расширения БЗ.

(2.2) *БЗ* – подсистема представления знаний.

Обычно выделяют три типа знаний для КС: декларативные, процедурные и концептуальные [6].

Под процедурными знаниями понимают задание алгоритмов и их комбинаций, применяемых в *Решателе* задач для достижения цели. Процедурным знанием являются стратегии решения задач, образованные посредством комбинирования различных видов, рассуждений и вычислений.

Под декларативным знанием понимают системы утверждений и, в частности, характеризацию предметной области (ПрО). Таковой являются аксиомы структуры данных (например, булевской) и дескриптивные утверждения, характеризующие предметную область (они могут быть необходимыми условиями корректности результатов применяемых процедур *Решателя* задач). Декларативным знанием ИС являются также утверждения, выражающие в импликативном виде правила вывода *Рассуждателя*. Эти утверждения образуют метатеорию ИС и создают возможность исследования на логическом уровне процедур *Рассуждателя*.

Концептуальным знанием ИС является множество утверждений и определений понятий, характеризующих принципы создания ИС.

Это знание является метатеоретическим, которым руководствуются создатели ИС.

(3) Интеллектуальный интерфейс включает в себя диалог (наилучший вариант – диалог на естественном языке), демонстрацию как результатов работы ИС, так и процесса их получения, графическое представление результатов, научение пользователя работе с ИС, поддержка интерактивного режима работы ИС.

Рассуждения и вычисления, представление знаний и интерфейс являются практическими реализациями принципов функционирования ИС. Посредством этих компонент функционирования ИС осуществляется интеллектуальная обработка данных.

Под «представлением знаний в ИС» понимают как выбор формы выражения знания посредством некоторого специального языка L, так и содержание, отображающего фрагмент предметной области, введенный в ИС в соответствии с целями, т.е. решаемыми задачами [8]. Наиболее известными формами представления знаний в ИС являются язык логики предикатов 1-го порядка, семантические сети и фреймы [7].

Утверждение 2. Самоорганизующаяся система $\mathcal{K}$ относится к классу Интеллектуальных Систем.

Доказательство:

Учитывая совокупность способностей, которыми должна обладать киберсистема, чтобы она могла быть отнесена к классу антиципирующих, а также детализацию процессов функционирования киберсистемы с упреждающим поведением [1], можно определить ряд параметров и отображений:

– $F_{ExtrW} : L_{SM} \times Z_M \to Z_{MeW}$, где Z_{MeW} – прогнозируемая модель наблюдаемого процесса (F_{ExtrW} – функция выявления типов потенциально возможных опасностей путем построения обобщенных моделей потенциально реализуемых атакующей стороной процессов);

– $Concl : Z_{MeW} \to C$, где C – оценка прогнозируемого процесса, наблюдаемого киберсистемой;

– $F_{ExtrS} : L_{SM} \times (Z_M \bigcup Z_{MeW}) \to Z_{MeS}$ – построение модели действий киберсистемы в условиях реализации прогнозируемого процесса, где Z_{MeS} – модель действий системы в ситуации Z_{MeW} (т.е. по результатам оценивания система должна быть способной принимать решения о том, какие ей необходимо осуществить действия для достижения потребного для нее и для защищаемой КИИ будущего; $F_{ExtrS} \subset F$);

– $F_{ExtrW} : L_{SM} \times (Z_M \cup Z_{MeS}) \to \overline{Z}_{MeW}$, где $\overline{Z}_{MeW}$ – прогнозируемая модель наблюдаемых процессов в условиях противодействия со стороны $\mathcal{K}$ (естественно предположить, что различные ответные действия интеллектуальной системы могут приводить к различным результатам, которые сама система должна заранее просчитывать);

– B – множество базовых элементов, через которые система сможет описывать предметную область конфликта;

– L – множество синтаксических правил построения более сложных структур, позволяющих описывать ПрО, используя B;

– $D = B \times L$, тогда $Pr : B \times L \times X_S \to L_{SM}$;

– Q – множество правил порождения киберсистемой новых знаний из имеющихся в конкретный момент (т.е. с учетом поступивших), $F_Q : Q \times Z_M \to Z_M$.

Лемма 2.1. Полнота и качество моделей упреждающего поведения в конфликте, формируемых системой $\mathcal{K}$, зависит от: имеющихся у нее знаний (Z_M), поступающих на ее вход(ы) данных (X), языка представления знаний (D) и правил порождения новых знаний из имеющихся (Q).

Доказательство:

$F_{ExtrW} : L_{SM} \times Z_M \to Z_{MeW}$ – потенциальная Задача (потенциально возможная опасность – см. [1]) – зависит от Z_M;

$F_{ExtrS} : L_{SM} \times (Z_M \cup Z_{MeW}) \to Z_{MeS}$ – потенциальное Решение (потенциально реализуемый вариант решения – см. [1]) – зависит от Z_M;

$F_Q : Q \times Z_M \to Z_M$, учитывая, что $M : L_{SM} \times Z_M \to Z_M$ и $Pr : B \times L \times X_S \to L_{SM}$, можно записать: $F_Q : Q \times B \times L \times X_S \times Z_M \to Z_M$, известно, что: $D = B \times L$, а $S : X \times T \to X_S$, тогда очевидно, что: полнота и качество моделей упреждающего поведения, зависящие от полноты и качества выявления потенциальных Задач (Z_{MeW}) и способов их потенциальных Решений (Z_{MeS}), зависят от Z_M, X, D и Q.

△ *Лемма 2.1.*

В таблице 1 приведено соответствие элементов интеллектуальной системы и функций, которые должны быть реализованы в проектируемой киберсистеме.

Таблица 1. Соотнесение элементов ИС и функций $\mathcal{K}$

ИС	Система $\mathcal{K}$
1 Решатель задач	
1.1 Рассуждатель	$D = B \times L$; $F_Q : Q \times Z_M \to Z_M$; $F_Q : Q \times B \times L \times X_S \times Z_M \to Z_M$;
1.2 Вычислитель	Вычислитель – частный случай Рассуждателя при соответствующем Q
1.3 Синтезатор	$F_{ExtrW} : L_{SM} \times Z_M \to Z_{MeW}$; $F_{ExtrS} : L_{SM} \times (Z_M \cup Z_{MeW}) \to Z_{MeS}$; $Concl : Z_{MeW} \to C$; $F_{ExtrW} : L_{SM} \times (Z_M \cup Z_{MeS}) \to \overline{Z}_{MeW}$; $D \times Z_{MeS} \to Y_S$;
2 Информационная среда	
2.1 База Фактов	L_{SM} ;
2.2 База Знаний	$M : L_{SM} \times Z_M \to Z_M$; Z_M ;
3 Интеллектуальный интерфейс	$S : X \times T \to X_S$; $Pr : B \times L \times X_S \to L_{SM}$; $R : Y_S \times T \to Y$

▲ *Утверждение 2.*

Дополнительные требования к системе порождения сценариев упреждающего поведения в конфликте: (1) при реализации «*Рассуждателя*» в проектируемой системе необходимо учесть возможность его применения к «открытым мирам», а следовательно, (2) База Фактов, представляющая предметную область конфликтов, должна быть способной представлять “открытый мир”.

Выдвинутые требования (1, 2) обусловлены тем, что проектируемая система должна быть потенциально способной формировать сценарии упреждающего поведения в новых типах конфликтов (сценарии, предотвращения которых не вносились непосредственно в систему при ее создании) – см. Лемму 1.3.

Требование (3): «*Синтезатор*» должен выбирать стратегии поведения, адекватные не только состоянию информационной среды, но и целям системы, которые могут изменяться в ходе ее функционирования.

Если рассматривать различные цели как различные контексты, оказывающие влияние на принятие того или иного решения, то можно предположить, что контекст должен оказывать влияние на доступность решений. Пусть Br_b – доступность базовых элементов, а Br_l – проводимость связей между элементами B, тогда можно определить: $AS : Q \times B \times L \times X_S \times Z_M \times Br\_b \times Br\_l \to Z_M \times Br\_b \times Br\_l$.

А.Пуанкаре, Р.Курант, Г.Роббинс, Д.Пойа и И.Лакатос в своих работах выделяли, что в математическом творчестве важную роль играет аналогия. Можно предположить, что механизм порождения новых знаний (осуществляемых *Решателем* задач), основанный на выводах по аналогии (для обнаружения «Задач» и поиска их «Решений»), может быть весьма полезным для системы $\mathcal{K}$ в ходе порождения сценариев упреждающего поведения в конфликте.

Пусть:

– $F_{Z\_WW} : Z_M \times Z_{MeW} \to Z'_{MeW}$;

– $F_{Z\_SW} : Z_M \times Z_{MeS} \to Z'_{MeW}$;

– Z'_{MeW} – модели “Задач”, найденные по аналогии;

– $F_{Z\_WS} : Z_M \times Z_{MeW} \to Z'_{MeS}$;

– $F_{Z\_SS} : Z_M \times Z_{MeS} \to Z'_{MeS}$;

– Z'_{MeS} – модели “Решений”, найденные по аналогии.

Очевидно, что обнаружить «Задачи» и найти их «Решения», используя вывод новых знаний только по аналогии, можно не всегда, так как в ИС могут отсутствовать необходимые знания. Ввиду этого, видится полезным реализовать в «Синтезаторе» возможность порождения новых знаний путем комбинирования имеющихся. Очевидно, что произвольное комбинирование может привести к “комбинаторному взрыву” и к порождению моделей абсурдных процессов, поэтому в ИС должен быть реализован механизм направленного комбинирования для формирования моделей потенциально реализуемых процессов (т.е. $Q \subset Rl$, где Rl – правила вывода одних синтаксически и семантически верных конструкций, описывающих модели процессов, из других).

Проектированием ИС, способных корректировать собственные модели поведения под влиянием факторов из «Внешнего Мира», занимались и ранее в рамках исследований в области Искусственного Интеллекта. Подобные системы относятся к классу гироматов.

6. Киберсистема, способная к упреждающему поведению в конфликте, – самообучающаяся интеллектуальная система самоорганизующихся гироматов. Само слово «гиромат» придумано польским писателем-фантастом С. Лемом. По Лему, гиромат – это интеллектуальная машина, способная обнаруживать вокруг себя изменения и быстро откликаться на новизну, обучаться, меняя свое строение, приспосабливаясь к миру. Иными словами, гироматами С.Лем называет автоматы, самостоятельно составляющие для себя программу и «самоусовершенствующиеся». Далее идею гироматов, как устройств,

обладающих способностью изменять в соответствии с обстоятельствами свою семиотическую модель внешнего мира, научно обосновал и развил в своих работах Д.А. Поспелов [9, 10].

Гиромат Д.А. Поспелова – элементарная модель целесообразного поведения, способная адаптироваться к условиям решаемой задачи – уже содержал следующие «агенто-образующие» модули: блок мотивации; блок селекции (рецепторы); блок построения внутренней модели внешней среды; блок выдвижения гипотез; блок модельного опыта; блок выработки решений; блок активного опыта; блок времени.

Общая идея работы гиромата изложена в работах [9, 10]. Необходимыми условиями реализации искусственным агентом (гироматом) некоторого поведения являются наличие специальных устройств, непосредственно воспринимающих воздействия внешней среды (рецепторов) и исполнительных органов, воздействующих на среду (эффекторов), а также процессора (блока переработки информации) и памяти. Под памятью понимается способность агента хранить информацию о своем состоянии и состоянии среды. Таким образом, исходное представление о простейшем агенте Д.А.Поспелов свел к модели «организм-среда», описанной в монографии [9].

Поскольку проектируемая киберсистема ($\mathcal{K}$) должна быть интеллектуальной многоагентной системой, то возникает вопрос, связанный с исследованием процессов коммуникации, кооперации и координации агентов. При этом следует понимать, что распределенные интеллектуальные системы могут иметь единый орган управления, а в децентрализованных системах управление происходит только за счет локальных взаимодействий. В обоих этих случаях интеллектуальные процессы должны рассматриваться в контексте коллективного поведения, а центральным объектом исследования тогда становится группа или сообщество саморазвивающихся гироматов.

В работе [11] В.Б.Тарасов изложил заслуживающие внимания основы системно-организационного подхода в искусственном интеллекте (ИИ), включающие в себя следующие главные принципы:

– исследования интеллекта в иерархии взаимодействующих систем, что означает целесообразность изучения метаинтеллектуальных процедур, которые определяют, например, нормы взаимоотношений агентов в многоагентных системах;

– учета коллективной природы интеллекта, что предполагает обращение к семиотическим аспектам интеллекта;

– определения рекурсивных связей между интеллектом и деятельностью, согласно которому интеллект агента выступает как под-

система управления деятельностью, позволяющая ему организовать свои действия или действия другого агента;

– невозможности решения сложных задач отдельными агентами, опирающимися на локальные модели;

– дополнительности различных моделей интеллекта (аналогичный принципу Н.Бора), согласно которому невозможно отразить в одной модели многомерный характер понятия интеллект; для этого требуется построение семейства взаимодополняющих моделей;

– выделения системных единиц интеллекта.

В основу системного синтеза распределенного (децентрализованного) интеллекта целесообразно положить формирование функционально-структурной единицы как «универсального строительного блока» или «клетки» многоагентной системы. Системные единицы следует отличать от элементов: структурный элемент - это простейшая, неделимая часть системы, которая обычно не сохраняет свойства системы как целого, тогда как важнейшим требованием к функционально-структурной единице является сохранение важнейших свойств организации всей системы.

Исходя из результатов вышеприведенных рассуждений, будем полагать, что искомая интеллектуальная система, способная к порождению спецификаций упреждающего поведения в конфликте, может быть представлена в виде иерархии взаимодействующих частично-упорядоченных гироматов.

Следует отметить, что иерархия взаимодействующих гироматов тоже есть гиромат, но обладающий более совершенными «агентообразующими» модулями по сравнению с отдельно взятыми гироматами, входящими в иерархию.

В целом же, проектируемая киберсистема должна быть в состоянии как обнаруживать потенциально опасные процессы – «Задачи», так и находить пригодные их “Решения”. Очевидно, что обладая пустой Базой Знаний, система будет не в состоянии решить поставленные задачи. Поэтому видится необходимым указать, что система для решения перечисленных выше задач должна обладать необходимым объемом исходных знаний. Точно определить необходимый и достаточный объем знаний априорно невозможно, так как априорно неизвестны конкретные задачи, которые могут возникнуть перед киберсистемой в ходе защиты КИИ.

7. Заключение. Можно предположить, что информационно-технические системы, обладающие свойством антиципации и способные синтезировать спецификации упреждающего поведения в конфликте, в скором будущем найдут широкое применение в области

обеспечения безопасности компьютерных систем, входящих в состав КИИ, а также и в других областях деятельности человека.

Очевидно, что синтез и применение антиципирующих систем упреждения атакующих воздействий (компьютерных атак), должны повысить уровень защищенности критической информационной инфраструктуры. Сами искомые системы должны быть реализованы в виде многоагентных интеллектуальных самоорганизующихся систем, которые могут быть представлены в виде иерархии взаимодействующих гироматов. Как видится, именно гироматы должны стать основой антиципирующих систем предотвращения рисков реализации киберугроз.

Литература

1. *Бирюков Д.Н., Ломако А.Г.* Подход к построению системы предотвращения киберугроз // Проблемы информационной безопасности. Компьютерные системы. 2013. №2. С. 13–19.
2. *Бирюков Д.Н.* Анализ способностей живых организмов при проектировании систем кибербезопасности // Методы обеспечения информационной кибербезопасности. Труды ИСА РАН. М.: КомКнига. 2013. Т. 27 (доп. выпуск). С. 431–446.
3. *Бирюков Д.Н., Ломако А.Г.* Построение систем информационной безопасности: от живых организмов к киберсистемам // Защита информации. INSIDE. 2013. №2. С. 2–6.
4. *Эшби У.Р.* Принципы самоорганизации // Принципы самоорганизации // М.: Мир. 1966. С. 314–343.
5. *Финн В.К.* Об интеллектуальном анализе данных // Новости Искусственного интеллекта. 2004. № 3. С. 3–18.
6. *Финн В.К.* Искусственный интеллект: Идейная база и основной продукт // Труды 9-ой национальной конференции по искусственному интеллекту. М.: Физматлит. 2004. Т. 1. С. 11–20.
7. *Jain S.* Systems That Learn // An Introduction to Learning Theory, second edition. The MIT Press. Cambridge. Massachusetts. London. England. 1999.
8. *Nilsson N.J.* Artificial Intelligence: A New Synthesis // Morgan Kaufmann Publishers. Inc. San Francisco. California. 1998. 513 p.
9. *Гаазе-Рапопорт М.Г.* От амебы до робота: модели поведения // М.: Наука. 1987. 286 с.
10. *Поспелов Д.А.* Мышление и автоматы // М.: Советское радио. 1972. 224 с.
11. *Тарасов В.Б.* Системно-организационный подход в искусственном интеллекте // Программные продукты и системы. 1999. №3. С. 6–13.

References

1. Biryukov D.N., Lomako A.G. [Approach to creation of system of cyber-threats preventing]. *Problemy informatsionnoy bezopasnosty. Kompyuternie sistemy – Problems of information security. Computer systems*. 2013. no. 2. pp. 13–19. (In Russ).
2. Biryukov D.N. [Analysis of the ability of living organisms in the design of systems cybersecurity]. *Metody obespeceniya informatsionnoy kiberbezopasnosty. Trudy ISA RAN – ISA RAS proceedings Methods of providing information cybersecurity.* M.: KomKniga. 2013. vol. 27 (add. issue). pp. 431–446. (In Russ).
3. Biryukov D.N., Lomako A.G. [Design and construction of information security from living organisms to cybersystems]. *Zashita informatiyi – Data protection. INSIDE*. 2013. no. 2. pp. 2–6. (In Russ).
4. Ashby W.R. [Principles of self-organization]. *Principy samoorganizacii – Principles of self-organization.* M.:Mir. 1966. pp. 314–343.

5. Finn V.K. [About data mining]. *Novosty isskustvennogo intellekta – Artificial intelligence news*. 2004. no. 3. pp. 3–18. (In Russ).
6. Finn V.K. [Artificial intelligence: a Conceptual framework and the main product]. *Trudy 9-oj nacional'noj konferencii po iskusstvennomu intellektu* [Proceedings of the 9th national conference on artificial intelligence]. M.: Fizmatlit. 2004. vol. 1. pp. 11–20. (In Russ).
7. Jain S. Systems That Learn. An Introduction to Learning Theory, second edition. The MIT Press. Cambridge. Massachusetts. London. England. 1999.
8. Nilsson N.J. Artificial Intelligence: A New Synthesis. Morgan Kaufmann Publishers. Inc. San Francisco, California. 1998. 513 p.
9. Gaaze-Rapoport M.G. *Ot ameby do robota: modeli povedenija* [From the amoeba to the robot: model behavior]. M.: Nauka. 1987. 286 p. (In Russ).
10. Pospelov D.A. *Myshlenie i avtomaty* [Thinking and machines]. M.: Sovetskoe radio. 1972. 224 p. (In Russ).
11. Tarasov V.B. [Systematic organizational approach in artificial intelligence]. *Programmniyi produkty i sistemy – Software and systems.* 1999. no. 3. pp. 6–13.

Бирюков Денис Николаевич — к-т техн. наук, профессор кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: системный анализ, защита информации, интеллектуальная поддержка принятия решений. Число научных публикаций — 70. Biryukov.D.N@yandex.ru; ул. Ждановская, д. 13, г. Санкт-Петербург, 197198; р.т.: (812) 237-19-60.

Biryukov Denis Nikolaevich — Ph.D., professor of systems for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: system analyses, IT-Security, intelligent decision support. The number of publications — 70. Biryukov.D.N@yandex.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: (812) 237-19-60.

Ломако Александр Григорьевич — д-р техн. наук, профессор кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: информационная безопасность, теоретическое и системное программирование, синтез и верификация корректности моделей программ. Число научных публикаций — 250. lomako_ag@mail.ru; ул. Ждановская 13, 197198, Санкт-Петербург; р.т.: +7(812) 237-19-60.

Lomako Aleksandr Grigor'evich — Ph.D., Dr. Sci., professor of system for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: information security, theoretical and system programming, synthesis and verification of program models. The number of publications — 250. lomako_ag@mail.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812) 237-19-60.

Ростовцев Юрий Григорьевич — д-р техн. наук, профессор, заслуженный деятель науки и техники Российской Федерации, заслуженный работник высшей школы Российской Федерации, профессор кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: системный анализ, теоритическая и прикладная кибернетика, методология знакового моделирования, радиотехника. Число научных публикаций — 350. Y.Rostovtsev@yandex.ru; ул. Ждановская 13, Санкт-Петербург, 197198; р.т.: +7(812) 237-19-60.

Rostovtsev Yuriy Grigorievich — Ph.D., Dr. Sci., professor, honored scientist and technology of Russian Federation, honored worker of higher school of Russian Federation, professor of systems for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: system analyses, theoretical and applied cybernetics, the methodology of symbolic modeling, radio engineering. The number of publications — 350. Y.Rostovtsev@yandex.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812) 237-19-60.

РЕФЕРАТ

Бирюков Д.Н., Ломако А.Г., Ростовцев Ю.Г. **Облик антиципирующих систем предотвращения рисков реализации киберугроз.**

На современном этапе развития средств обеспечения информационной безопасности назрела объективная необходимость создания систем, способных осуществлять предупреждение и заблаговременное пресечение компьютерных атак на защищаемые ресурсы. Так же можно наблюдать, что в области безопасности компьютерных систем и сетей с каждым днем все чаще упоминаются и рекламируются различные биоинспирированные подходы, основанные на биологической метафоре. В развитии биоинспирированных подходов предлагается наделить комплексные средства обеспечения информационной безопасности принципиально новым свойством, позволяющим им предвидеть развитие событий, явлений, результатов действий и готовиться к ним. Такое свойство называется “Антиципация”.

В работе обоснованы основные задачи, решение которых должно позволить киберсистеме осуществлять предотвращение компьютерных атак. Определено, что система, способная предотвращать компьютерные атаки, должна относиться к классу интеллектуальных самоорганизующихся систем и быть представлена в виде иерархии взаимодействующих гироматов.

SUMMARY

Biryukov D.N., Lomako A.G., Rostovtsev Y.G. **The Appearance of Anticipating Cyber Threats Risk Prevention Systems.**

At the present stage of development of information security there is objective necessity of developing systems capable of carrying out prevention and early prevention of cyber attacks on protected resources. You can also observe that the security of computer systems and networks with each passing day more and more often mentioned and advertised bioinspired different approaches based on biological metaphor. In the development of bioinspired approach the means of the complex information security to endow are offered by fundamentally new feature that allows them to anticipate developments, events, results of operations and prepare for them. This property is called "Anticipation".

In work the main objectives, which decision has to allow cybersystem to carry out prevention of computer attacks, are proved. It is defined that the system capable to prevent computer attacks has to belong to the class of the intellectual self-organizing systems and to be presented in the form of hierarchy of the interacting gyromats.