ПРИМЕНЕНИЕ ЛОГИКО-ВЕРОЯТНОСТНОГО МЕТОДА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ЧАСТЬ 2)

Калашников А.О.[1], Бугайский К.А.[2], Аникина Е.В.[3], Перескоков И.С.[4], Петров Ан.О.[5], Петров Ал.О.[6], Храмченкова Е.С.[7], Молотов А.А.[8]

Цель исследования: *адаптация логико-вероятностного метода оценивания сложных систем к задачам построения систем защиты информации в многоагентной системе.*

Метод исследования: *при проведении исследования использовались основные положения методологии структурного анализа, системного анализа, теории принятия решений, методов оценивания событий при условии неполной информации, логико-вероятностных методов.*

Полученный результат: *данная статья продолжает рассмотрение вопросов информационной безопасности на основе анализа отношений между субъектами и объектом защиты. Обосновано представление субъекта и объекта защиты в виде интелектуального агента с учетом требований по защите информации. Даны формальные определения агента информационной безопасности и его основных характеристик: информационный ресурс, информационный поток и права доступа субъекта. Показано, что понятие агента информационной безопасности представляет собой основу для описания структур в информационной системе. Разработана аксиоматика отношений субъекта и объекта как агентов информационной безопасности, а также отношений между информационными ресурсами и информационными потоками внутри агента. Показана возможность определения состояния агента на основе формируемых в процессе его функционирования событий и сообщений.*

Научная новизна: *рассмотрение вопросов защиты информации с использованием аппарата математических и логических отношений. Разработка формальных определений агента информационной безопасности и составляющих его информационных ресурсов и информационных потоков, являющихся базовыми универсальными компонентами описания структур в информационной системе. Определение понятия агента информационной безопасности за счет рассмотрения отображения субъекта и его целеполагания на объект.*

Вклад авторов: Калашников А. О. *выполнил постановку задачи и общую разработку модели применения логико-вероятностного метода в информационной безопасности;* ***Бугайский К.А., Аникина Е.В.*** *разработали модель описания проблем информационной безопасности через отображение субъекта и его целеполагания на объект, а также типы и аксиоматику отношений агентов;* ***Перескоков И.С*** *и* ***Петров Андрей О.*** *разработали модель отображения субъекта на объект;* ***Петров Александр О.*** *и* ***Храмченкова Е.С.*** *разработали модель отображения целеполагания субъекта на объект;* ***Молотов А.А.*** *разработал модель формирования событий и сообщений агента.*

Ключевые слова: *модель информационной безопасности, оценка сложных систем, теория отношений, системный анализ, многоагентная система.*

DOI:10.21681/2311-3456-2023-5-113-127

1 Калашников Андрей Олегович, доктор технических наук, главный научный сотрудник лаборатории «Сложных сетей» ФГБУН Институт управления имени В.А. Трапезникова РАН, г. Москва, Россия. E-mail: aokalash@ipu.ru

2 Бугайский Константин Алексеевич, младший научный сотрудник Института проблем управления имени В.А. Трапезникова РАН, г. Москва, Россия. E-mail: kabuga@ipu.ru

3 Аникина Евгения Владимировна, научный сотрудник Института проблем управления имени В.А. Трапезникова РАН, г. Москва, Россия. E-mail: ajanet@ipu.ru

4 Перескоков Илья Сергеевич, младший научный сотрудник Института проблем управления имени В.А. Трапезникова РАН, г. Москва, Россия. E-mail: pereskokov@phystech.edu

5 Петров Андрей Олегович, младший научный сотрудник Института проблем управления имени В.А. Трапезникова РАН, г. Москва, Россия. E-mail: petrovaojob@gmail.com

6 Петров Александр Олегович, младший научный сотрудник Института проблем управления имени В.А. Трапезникова РАН, г. Москва, Россия. E-mail: petrovalexandr@ipu.ru

7 Храмченкова Екатерина Сергеевна, младший научный сотрудник Института проблем управления имени В.А. Трапезникова РАН, г. Москва, Россия. E-mail: hramchenkovaes@yandex.ru

8 Молотов Александр Анатольевич, инженер-программист Института проблем управления имени В.А. Трапезникова РАН, г. Москва, Россия. E-mail: alpha.sphere@ya.ru

Введение

Данная статья является второй из серии публикаций, посвященных исследованию вопроса применения логико-вероятностного метода при изучении вопросов защиты информации. Метод был разработан Рябининым И.А. [1, 21]. Метод получил высокую популярность при проведении исследований, связанных с анализом и оценкой сложных систем. Прежде всего для решения вопросов надежности работы систем и причин возникновения аварийных ситуаций. Логико-вероятностный метод предполагает решение следующих задач.

1. Построение структурно-логической модели системы за счет выделения и использования событий с несовместными исходами.

2. Проведение преобразований полученных логических уравнений на основе функций булевой алгебры с целью получения системы уравнений с конечным числом переменных.

3. Теоретически обоснованный переход от уравнений булевой алгебры к уравнениям с вероятностными переменными.

К несомненным достоинствам логико-вероятностного метода следует отнести его способность обеспечить прозрачность процедур анализа и оценки сложных систем, а также хорошие адаптационные способности к новым задачам. Результатом применения логико-вероятностного метода являются количественные оценки риска как вероятности нарушения работоспособности системы. Интерес к логико-вероятностному методу – помимо типичных вопросов надежности систем, – в настоящее время подкрепляется исследованием задач машинного обучения и связанных с ними проблем оптимизации расчетов [см., например, 2-5]. В частности, логико-вероятностный метод обеспечивает хорошую точность и стабильность результатов в задачах распознавания объектов. Логико-вероятностный метод также находит свое применение при решении задач защиты информации [см., например, 6-11].

Тем не менее, представляется, что логико-вероятностный метод обладает значительно большим, пока не раскрытым, потенциалом в случае его дальнейшего развития и адаптации к решению задач в области информационной безопасности (далее – ИБ).

Постановка задачи

Современные информационные системы (далее – ИС) [12, 13] отличаются большим разнообразием обрабатываемой информации, сложными типами связей между аппаратными и программными компонентами, распределенным характером обработки и управления информацией и компонентами ИС. Что с большой вероятностью влечет за собой проблему экспоненциального взрыва при непосредственном использования для описания структурно-логических схем ИС функций алгебры логики в рамках логико-вероятностного метода. Вместе с тем, логико-вероятностный метод содержит теоретические положения, позволяющие заместить систему логических равенств описывающих структурно-логическую схему одним равенством.

В рамках достижения общей цели исследования (адаптации логико-вероятностного метода для решения задач ИБ) в настоящей статье разработаны формально-логические основы для определения и последующего выделения фрактальных структур, присущих ИС как сложной системе. Для решения этой задачи выделяется макроуровень ИС, состоящий из агентов информационной безопасности и проводится рассмотрение отношений между ними.

Определение агента ИБ

Объектом в отношениях «субъект-объект» для Защитника и Нарушителя, определенных в первой части настоящей работы, является ИС, представленная в виде графа $G(V,E)$. На основании [14, 15] можно сказать, что выполнение действий субъектом невозможно без функционала, обеспечивающего отображение как целей субъекта на объект, так и собственно субъекта на объект. Исходя из того, что в каждый конкретный момент времени субъект взаимодействует с определенной компонентой ИС, то в качестве объекта в отображениях следует принять узел ИС. Сам факт существования указанных отображений позволяет при рассмотрении вопросов защиты информации предположить условное наличие «ограниченной субъектности» узлов ИС.

Рассмотрим эти отображения на основе категориального подхода и с учетом положений и выводов, изложенных в [13, 16, 17, 18]

Отображение субъекта на объект. Существующая парадигма ИБ предполагает рассмотрение этого отношения с точки зрения возможностей (прав) субъекта *AS* по использованию ресурсов объекта – ИС, представленной графом $G(V,E)$. Каждый узел графа описывается ресурсами $V[\![Res]\!]$, которые могут быть представлены набором, состоящим из перечня данных, обрабатывающих их программ и кон-

фигураций, обеспечивающих правила обработки $Res = \{Data, Prog, Conf\}$. В рамках существующих архитектурных решений операционных систем компонент ИС субъект может быть представлен только в виде аккаунта *AC* пользователя операционной системы данного узла, который манипулирует данными $Data$ с помощью программ $Prog$. Поскольку ресурсы заданы изначально, это означает, что для функции распределения ресурсы узла являются областью определения, а аккаунт – областью назначения. При этом данные могут рассматриваться как область определения для программ. Если ввести отношение «больше» в описание узла $V[\![Data, Prog, AC, >]\!]$, то получаем выражение для отображения субъекта на объект:

$$AS \xrightarrow{Res} V : Data \to Prog \to AC \to AS \qquad (1).$$

Деятельность субъекта в рамках аккаунта *AC* и функционирование программ *Prog* формируют события и сообщения *ME* на узле. Для ИС и ее компонент целесообразно рассматривать сообщения и ошибки как часть данных узла: $ME \subset Data$. Что позволяет определить отношения $ME \to AC \wedge ME \to Prog$. Коммутационная диаграмма отображения субъекта на объект приведена на рисунке 1.

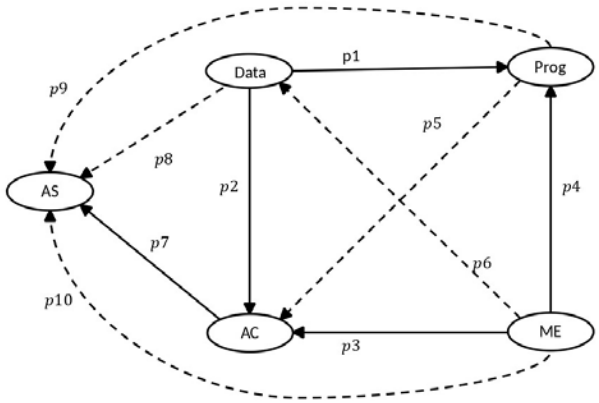

Рис. 1. Диаграмма отображения субъекта на объект

На этом и последующих рисунках сплошными стрелками обозначены отношения явно сформулированные при описании отображения. Пунктирные стрелки обозначают отношения, являющиеся следствием коммутативности диаграммы.

Отображение целей субъекта на объект. В общем случае при нормальном функционировании узел ИС выполняет правила, которые определяются субъектом и по сути являются отображением его целей на графе $G(V, E)$. Для Защитника целеполагание может быть представлено как набор отдельных целей достижимых на различных узлах $\overline{GS} = \bigcup_V \overline{g_v}$, $v \in V$. В случае успешных действий Нарушителя узел может также реализовывать и задаваемые им цели – $GS = \bigcup_V g_v$, $v \in V$. Обозначим итоговое целеполагание узла $GG = (\overline{g_v} \wedge g_v)$. Положим, что реализация целей g_v и $\overline{g_v}$ требует выполнения определенных правил функционирования ресурсов узла – *Conf*. Целесообразно считать, что целеполагание является первоочередным в деятельности субъекта и у него может быть несколько целей. Кроме того, положим, что для достижения конкретной цели субъект может использовать различные комбинации правил функционирования программ и аккаунта узла – конфигурации. Следовательно, можно записать отображение как:

$$AS \xrightarrow{GG} V : GG \to AS \wedge Conf \to GG \qquad (2).$$

С точки зрения архитектуры современных ИС и их компонент, узел графа $G(V, E)$ должен предоставлять пути доступа (*AP*) к своим ресурсам. Под путями доступа будем понимать различные комбинации программных интерфейсов (API), портов и протоколов, применяемых ресурсами узла как для доступа субъектов к аккаунтам, так и для обмена информацией с другими узлами в процессе функционирования.

Доступ субъекта к ресурсам узла через аккаунт должен осуществляться посредством пути доступа. Современные операционные системы обладают свойством предоставлять несколько путей доступа к ресурсам узла. Соответственно, субъект для доступа к ресурсам узла может выбрать один из существующих путей доступа, то есть речь идет об отображении: $AP \to AS$.

Коммутационная диаграмма отображения целей субъекта на объект приведена на рисунке 2.

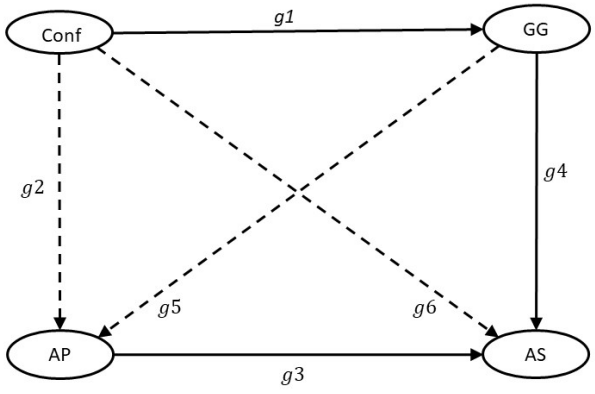

Рис. 2. Диаграмма отображения целей субъекта

На диаграмме выделим морфизм $g6 = g4 \circ g1$, представляющий собой выражение (2).

Полное отображение субъекта на объект. Построение коммутационной диаграммы полного отображения субъекта на объект необходимо и возможно на основании того, что пути доступа и конфигурации должны быть соотнесены с объектом – узлом ИС. На основании анализа деятельности Нарушителя, по разделу тактик, техник и процедур базы знаний организации MITRE (mitre.org) можно говорить, что получение доступа к узлу по любому из путей дает возможность оперировать с множеством ресурсов узла. Таким образом, речь можно вести речь о признании аккаунтов и программ узла областью определения для пути доступа: $AC \to AP \wedge Prog \to AP$.

Архитектура современных операционных систем обеспечивает доступ с одного аккаунта не только к нескольким программам, но и к нескольким конфигурациям. Что дает основания считать конфигурации областью определения аккаунта: $Conf \to AC$.

Полное отображение субъекта на объект в виде коммутационной диаграммы представлено на рисунке 3.

Отношение $Conf \to Prog$ (s1) вытекает из морфизмов $s3 = p4 \circ s1$ и $g2 = s2 \circ s1$.

На диаграмме отметим морфизм $s6 = g3 \circ s4$, подтверждающий выражение (1).

В первой части статьи было показано, что функционирование узла может быть представлено импликацией: $G(V,E) \to Res \to SA \to ME$. В свою очередь, события и сообщения оказывают решающее воздействие на выбор дальнейших действий субъекта: $ME \to SA \to Res$. Диаграммы отображения субъекта на объект (рисунок 1) и полного отображения (рисунок 3) позволяют дать следующее определение

Def. 1. Допустимые действия субъекта SA. Это такие действия субъекта, которые позволяют проводить необходимые ему манипуляции с данными, конфигурациями, событиями и сообщениями в рамках действующего аккаунта. Что можно формализовать в виде:

$$SA = (p9 \vee s6 \circ p4) \to (p1 \vee p6 \vee s1) \quad (3)$$

В результате построения коммутационных диаграмм полное описание узла принимает вид:

$$V[\![\ Prog, Conf, Data, ME, AP, AC, GG, AS,\ \cup_{i=[1,10]} p_i, \cup_{j=[1,6]} g_j, \cup_{k=[1,6]} s_k]\!] \quad (4).$$

Данное описание позволяет ввести следующие определения, которые будут формализованы как функционалы.

Def. 2. Права доступа. Права доступа субъекта к ресурсам определяются коммутационной диаграммой, приведенной на рисунке 4. Данная диаграмма построена на основании следующих морфизмов, определяющих права доступа:

$p2 = p5 \circ p1$ – соответствующий соотношению между данными, программами и аккаунтом (см. рисунок 1);

$p9 = p7 \circ p5$ – соответствующий использованию субъектом программ (см. рисунок1);

$s3 = p4 \circ s1$ – соответствующий соотношению между конфигурациями, программами и аккаунтом (см. рисунок 3);

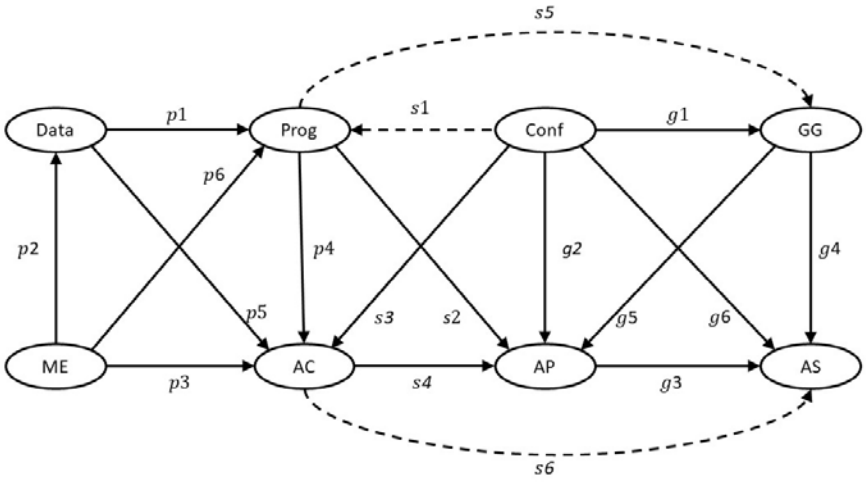

Рис. 3. Диаграмма полного отображения субъекта на объект

$s6 = g3 \circ s4$ – подтверждающий выражение (1), а также необходимость и достаточность представления аккаунта как отображения субъекта на узле (см. рисунок 4).

Указанные морфизмы дают функцию субъекта:

$$AR(AS) = (p1 \circ p9 \vee p2 \circ s6) \wedge \wedge (p9 \circ s1 \vee s6 \circ s3) \quad (5)$$

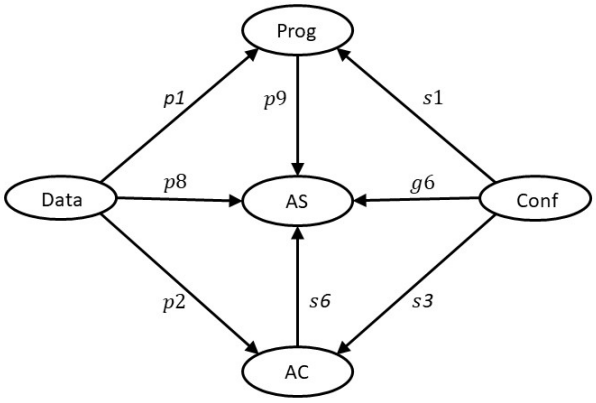

Рис. 4. Диаграмма прав доступа

Необходимо обратить внимание на наличие оператора ИЛИ в каждой из скобок выражения (5). Его наличие может свидетельствовать о *неполноте классических моделей*, рассматривающих проблему доступа «субъект-объект» в терминах «человек» и «данные». Данный вопрос заслуживает отдельного исследования.

Def. 3. Информационный ресурс. Под информационным ресурсом (далее – ИР) будем понимать набор данных и средств их обработки (программы). Диаграмма ИР представлена на рисунке 1 и как левая часть на рисунке 3.

$$IR = \{\bigcup_{i=[1,10]} p_i, AR(AS)\} \quad (6)$$

Def. 4. Информационный поток. Под информационным потоком (далее – ИП) будем понимать набор путей доступа к ресурсам узла со стороны субъекта или другого узла. Диаграмма ИП представлена центральной и правой частями на рисунке 3.

$$IS = \{\bigcup_{k=[1,6]} s_k, \bigcup_{j=[1,3]} g_j, \bigcup_{j=[5,6]} g_j, AR(AS)\} \quad (7)$$

Отметим, что в выражении (7) отсутствует морфизм: $g_4: GG \rightarrow AS$ в виду его имманентности.

Выражения (1 – 7) позволяют установить соотношения между понятиями «субъект», «аккаунт», «информационный ресурс» и «информационный поток» в виде орграфа как показано на рисунке 5.

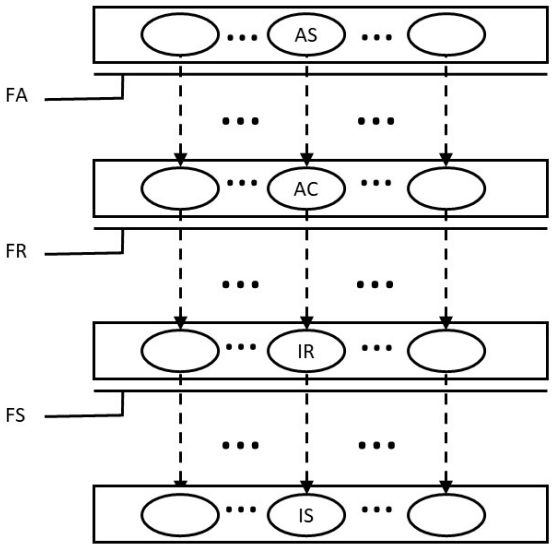

Рис. 5. Соотношения понятий

На рисунке связи орграфа показаны условно для сохранения наглядности и отображают только направление взаимодействия между понятиями. В реальности, например соотношение между аккаунтом и ИР как правило будет «один ко многим». В силу архитектуры ИС и компонент ИС соотношения между понятиями на каждом из трех уровней, обозначенные на рисунке как *FA*, *FR*, *FS* образуют иерархию. Это дает возможность рассматривать *FA*, *FR*, *FS* как функции связей для двудольных графов, образуемых *AS, AC, IR, IS*.

Обозначим:

e_1 – вершина верхнего уровня двудольного графа;

e_2 – вершина нижнего уровня двудольного графа;

$x(e_1, e_2)$ – связь между вершинами двудольного графа.

$$y = f(x) = \begin{cases} 1, \exists x(e_1, e_2) \\ 0, \nexists x(e_1, e_2) \end{cases}$$

Тогда можем записать:

$$FA(AC) = \langle y_1, \ldots, y_n \rangle, e_1 \in AS, e_2 \in AC, n = |AC|$$
$$FR(IR) = \langle y_1, \ldots, y_n \rangle, e_1 \in AC, e_2 \in IR, n = |IR|$$
$$FS(IS) = \langle y_1, \ldots, y_n \rangle, e_1 \in IR, e_2 \in IS, n = |IS|$$

При условии фиксации каждой из вершин верхнего уровня функции будут представлять собой бинарные вектора. В итоге узел ИС для конкретного субъекта может быть представлен как списки ИР доступных данному аккаунту и соответствующих ресурсу ИП:

$$V[\![AR(AS), FA(AC), FR(IR), FS(IS)]\!] \quad (8)$$

Одним из основополагающих принципов построения архитектуры узлов ИС является наличие для всех субъектов нестрогого порядка аккаунтов определяемого правами доступа $AC = \{ac_1, \ldots, ac_n, \leq_{AR}\}$,

$n = |AC|$. С этой точки зрения *FA*, *FR*, *FS* формируют граф подчиненности аккаунтам, который является графом со слабыми связями, то есть такой, в котором нижележащий узел связан с более чем одним узлом верхнего уровня.

Одним из основополагающих требований ИБ является установление категорий данных на основе определения их ценности для субъекта. При этом категории данных:

- представляют собой меру «абсолютной ценности» данных для субъектов (в настоящем исследовании не рассматривается);
- едины для всех субъектов и их аккаунтов в пределах конкретного объекта (например, узла ИС);
- отображаются на аккаунты в отношении «многие к одному», то есть один аккаунт может работать с несколькими категориями данных.

Обозначим множество категорий данных как Ξ и введем отношение строгого упорядочивания прав доступа по категориям данных $AR = \{ar_1, \dots, ar_n, <_\Xi\}$, $n = |\Xi|$.

Поскольку целью деятельности субъекта является обработка данных, а аккаунты, ИР и ИП являются средствами для этого, то можно считать, что эти средства также могут быть упорядочены по категориям данных. Но с учетом нестрогого порядка аккаунтов и подчиненности функций *FA*, *FR*, *FS* аккаунту, множества *AC*, *IR*, *IS* следует считать частично упорядоченными. То есть, каждый из элементов этих множеств может использоваться для обработки различных категорий данных. Тогда имеем:

$$AC = \{ac_1, \dots, ac_n, \leq_\Xi\}, n = |\mathrm{AC}|,$$
$$IR = \{ir_1, \dots, ir_n, \leq_\Xi\}, n = |\mathrm{IR}|,$$
$$IS = \{is_1, \dots, is_n, \leq_\Xi\}, n = |\mathrm{IS}|.$$

Морфизмы *s6* и *s5* позволяют сделать утверждение, что аккаунт, используемый субъектом для обработки данных определенной категории, может быть отождествлен с достижением конкретной цели. Это утверждение может быть представлено как морфизм: $AC \to GG$. Истинность этого морфизма подтверждается следующими выражениями (см. рис. 3) $Prog \to GG = (AC \to GG) \circ (Prog \to AC)$ и $AC \to AP = (AC \to GG) \circ (GG \to AP)$. При этом, каждое из выражений содержит морфизмы из определения ИП и ИР. Таким образом можно говорить об иерархии целей и средств их достижения в рамках аккаунта.

Обозначим:

$AC^\Xi, AC^\Xi \in AC$ – подмножество аккаунтов, используемых при обработке определенной категории данных для достижения заданной цели;

$IR^\Xi, IR^\Xi \in IR$ – подмножество ИР, используемых при обработке определенной категории данных для достижения заданной цели;

$IS^\Xi, IS^\Xi \in IS$ – подмножество ИП, используемых при обработке определенной категории данных для достижения заданной цели.

Тогда выражение (8) можно записать как

$$V = \bigcup_i (AC_i^\Xi, FR(IR_i^\Xi), FS(IS_i^\Xi)), i = [1, |\Xi|] \quad (9)$$

Иерархия целей обработки основана на категории данных и представляет собой решетку. Тогда, следуя [19, см. литературу там же], на основе категории данных можно сформировать подмножества множества путей, которые представляют собой цепочки связей от верхнего уровня иерархии к нижнему в графе подчиненности. То есть, фиксация (обозначаемая как $\hbar$) определенных аккаунта и категории данных формирует подмножество множества путей графа подчиненности.

$$ISA = ac_i^\Xi, FR(IR_i^\Xi), FS(IS_i^\Xi)$$
$$\hbar\, i \in \Xi, \hbar\, ac^\Xi \in AC^\Xi \quad (10)$$

Все современные компоненты ИС реализуют многопользовательский и многозадачный режим работы узлов обеспечивающий:

- взаимодействие между компонентами за счет обмена данными и сигналами, в том числе без участия субъекта;
- целенаправленную обработку данных с возможностью вариации имеющихся алгоритмов для разных типов данных;
- совместное использование своих ресурсов в зависимости от взаимодействия с субъектами и другими компонентами;
- оптимальность использования своих ресурсов зависимости от взаимодействия с субъектами и другими компонентами.

Опираясь на положения [20] совместно с выражениями (6 – 10) дадим следующее определение:

Def. 5. Агентом ИБ (information security agent – *ISA*) называется представление субъекта как аккаунт узла ИС, обеспечивающего ограниченно-рациональное и ограниченно-интеллектуальное использование доступных информационных ресурсов и информационных потоков узла для обработки определенной категории данных в интересах субъекта. Ограниченность

свойств рациональности и интеллектуальности определяется встроенными алгоритмами и конфигурациями узла.

С целью упрощения дальнейшего изложения введем следующие обозначения для ИП, входящих в состав агента – *QR* и для ИР из состава агента – *QS*.

Генерация событий и сообщений

Как было показано на коммутационной диаграмме отношений «субъект-объект» (рисунок 1), ИС является единственным источником доступных субъектам событий и сообщений *ME*. Собственно события и сообщения для субъектов формируются непосредственно узлами ИС, что выражается функцией *Gen(ME)*. Фактически речь идет о функции регистрации параметров работы каждого из агентов ИС. С учетом диаграммы полного отображения субъекта на объект через отношения: $Prog \to ME$, $AC \to ME$ и $Conf \to ME$ и соответствующие морфизмы можно записать:

$$Gen(ME) = p6 \vee p3 \vee \big((s3 \circ p3) \vee (s1 \circ p3)\big) = p6 \vee p3 \vee (s3 \vee s1) \quad (11)$$

Морфизм $AC \to ME$ соответствует регистрации действий субъекта в рамках аккаунта. В процессе реализации отношения формируются сообщения и события о фактах использования субъектом программ, данных и конфигураций, а также об ошибках при доступе и выполнении действий. Можно положить, что все ошибки для данного отношения так или иначе связаны с отказом в доступе конкретному субъекту $as \in AS$ к объектам *Prog*, *Conf*, *Data* через аккаунт $ac \in AC$ данного агента.

Морфизм $Conf \to ME$ соответствует регистрации фактов обращения к конфигурациям. Отметим, что все операции с конфигурациями – чтение, модификация, создание и удаление – совершаются с помощью программ. Кроме того, формирование ошибочных правил в конфигурациях ведут к ошибкам в работе программ.

Морфизм $Prog \to ME$ соответствует регистрации фактов использования программ. К которым относятся не только их запуск и останов, но и регистрация режимов обработки данных (возможно, и типов обрабатываемых данных). Сюда же целесообразно отнести сообщения о текущем статусе программ, которые могут включать описание программы в виде версии, подключенных модулях и т.п.

В общем виде функционирование агента в виде шагов приводящих к формированию событий и сообщений представлено на рисунке 6. Связь между «ME» и «старт обработки» показывает, что формирование сигналов и сообщений не прерывает обработку данных. Прерыванию обработки соответствует «сбой работы».

События и сообщения формируются внутри программ, – на основе их собственных параметров χ_i описывающих как обработку данных, так и состояние аппаратных средств. В общем виде формирование события или сообщения можно рассматривать как результат решения SMT-формулы (*satisfiability modulo theories*, SMT): $f\{\chi_{1,..,}\chi_i\} = true$. Отличительной особенностью SMT-формулы является наличие в ее составе количественных неравенств, результат вычисления которых дает значения «истина» или «ложь». Задача разрешения SMT-формул относится к NP-полным задачам, что может сказываться на достоверности и полноте формируемых событий и сообщений.

Таким образом, формирование событий и сообщений может быть представлено в общем виде как: $f\{\chi_{1,..,}\chi_i\} \to me, me \in ME$. Отметим, что решение

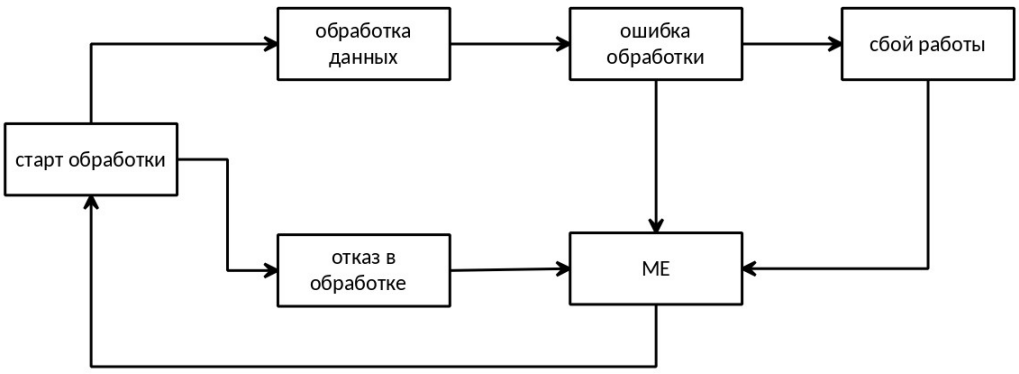

Рис. 6. Формирование ME

SMT-формулы дает только истинностное значение, а собственно событие или сообщение представляют из себя некоторую семантическую конструкцию пригодную для дальнейшей обработки. Это означает, что:

а) перечень событий и сообщений формируется разработчиками ИП и ИР и является конечным предопределенным множеством;

б) для каждого ИП и ИР определено собственное (уникальное) множество событий и сообщений;

в) решение SMT-формулы сопровождается выбором определенного события или сообщения из соответствующего множества $me = s(ME)$;

г) процедура выбора также определена разработчиками ИП и ИР.

Отметим, что механизмы формирования собственных параметров χ_i, наборов событий и сообщений, а также их соотнесение друг с другом для любого ИП и ИР не являются целью настоящего исследования.

Также отметим, в качестве промежуточного вывода, что:

1) функция генерации событий и сообщений может быть представлена в виде $Gen(ME): f\{\chi_{1,\dots,}\chi_i\} \to s(ME)$;

2) функция генерации событий и сообщений уникальна для каждого ИП или ИР $Gen(ME_i) \neq Gen(ME_j), i,j \in (QS \vee QR)$.

Введем функцию генерации событий и сообщений для конкретного ИП или ИР как $FE(x) : f\{\chi_{1,\dots,}\chi_i\} \to s(ME_x), \quad x \in (QS \vee QR)$. Результатом работы функции $FE(x)$ является подмножество выявленных в процессе работы событий ИП или ИР $M = FE(x)$ множества всех предопределенных событий и сообщений этого ИП или ИР ME_x, $M \subset ME$.

События и сообщения являются необходимыми исходными данными для субъекта при проведении им оценки агента, что позволяет определить в соответствии с выражением (10) новое множество, описывающее состояние агента на основании работы ИП и ИР из состава данного агента

$$QM = (\bigcup_{i \in QS} FE(QS_i)) \cup (\bigcup_{j \in QR} FE(QR_j)) \quad (12)$$

Рассуждения и выводы, позволившие сформулировать выражение (12), позволяют представить описание состояния агента посредством фиксированных наборов событий и сообщений – паттернов, которые представляют из себя подмножества множества *QM*, то есть: $QP = \{m_i, \dots, m_n\}, \ n = |QP|, \ m \in QM, \ QP_i \cap QP_j \neq \emptyset, QP_i \cup QP_j = QM$.

Соответственно можно определить функцию, определяющую вхождение события или сообщения в состав паттерна $FP(m): (m \in QM) \to (m \in QP)$. Результатом работы функции будет вектор, каждый элемент которого будет представлять из себя двоичную величину $BP = FP(QM), \ BP = \{b_i, \dots, b_n\}$, $b_i = \{0,1\}$. Значение «1» для элемента будет означать вхождение события или сообщения в паттерн. Отметим, что паттерн и соответствующий ему вектор будут формироваться каждым ИП и ИР из состава агента. Это дает основание говорить, что соответствующие вектора и множества описывают ИП и ИР: $QS[\![QP, BP]\!]$, $QR[\![QP, BP]\!]$. Представляется целесообразным положить, что в общем виде каждому состоянию агента будет соответствовать определенный паттерн *QP* и вектор *BP* для каждого ИП и ИР. То есть для определения состояния агента необходимо вычислить логическую функцию выполнения паттерна: $\psi = QP \wedge BP$, а затем уже определять состояние агента на основании функции

$$Ref: (\bigcup_{i \in QS} \psi_i) \cup (\bigcup_{j \in QR} \psi_j) \quad (13).$$

Таким образом, состояние агента будет считаться определенным, если $Ref = true$.

Следует отметить, что в процессе работы агента результаты вычислений функции ψ для отдельных паттернов того или иного ИП или ИР могут изменяться в силу того, что регистрируемые события и сообщения $m \in QM$ будут нести один из следующих видов информации:

- новое *m* подтверждает изменение параметров работы;
- новое *m* содержит ошибочные параметры;
- новое *m* является повторением имевшего место ранее;
- новое *m* не изменяет результатов.

То есть, следует вести речь о накоплении определенного количества изменений в текущем состоянии для перехода агента в иное состояние. Таким образом, целесообразно рассматривать функции определения состояния агента как функции времени $\psi(t)$ и $Ref(t)$. Детальное исследование механизма оценки состояния агента – функции *Ref* – будет проведено в следующей статье данного цикла статей. Выражения (9 – 10) показывают, что обработка данных в ИС может быть представлена через взаимодействие агентов. Для дальнейшего рассмотрения вопросов взаимодействия агентов необходимо определить типы их состояний

Состояния агента

В самом общем виде состояние агента можно рассматривать с двух точек зрения: что он знает о себе

(внутренняя оценка) и что агент знает о своем окружении (внешняя оценка). Подчеркнем еще раз, что единственным источником, позволяющем оценить состояние агента и его окружения, являются события и сообщения формируемые в результате обработки информации внутри данного агента в процессе его взаимодействия с этим окружением.

Архитектурные решения современных ИС основаны на взаимодействии их компонент в процессе обработки информации. В ИБ принято, как правило, рассматривать взаимодействие с точки зрения нарушения конфиденциальности, целостности и доступности данных. Без потери общности нарушение конфиденциальности, целостности и доступности можно отождествить с нарушениями работоспособности и/или прав доступа. Что может быть вызвано как внешним воздействием (атакой), так и внутренними причинами. На основании выражений (9 – 13) можно говорить о нарушениях конфиденциальности, целостности и доступности для ИП и ИР агентов, образующих ИС. Таким образом, внутренняя и внешние оценки состояний агента следует рассматривать с точки зрения его отношения к своему окружению – взаимодействующим агентам. Причем такие оценки состояния необходимо проводить для каждого из агентов окружения.

Прежде всего выделим состояние, когда внутри агента не фиксируется нарушений при взаимодействии с окружением. Это можно назвать состоянием *Лояльности* (*Lr*) – когда взаимодействующий агент осуществляет корректное, благожелательное сотрудничество, подразумевающее отсутствие намерений по нанесению ущерба оценивающему агенту.

Фиксация агентом нарушений своей работоспособности на основе собственных событий и сообщений позволяет определить состояние *Нелояльности* (*Dr*) – когда действия другого агента влекут за собой или могут расцениваться как подразумевающие нанесение ущерба агенту, производящему такую оценку. Здесь принципиально отметить следующую особенность. Если в процессе деструктивного воздействия агент оказывает противодействие, то это следует расценивать как стремление нанести ущерб атакующему. Следовательно, для атакующего защищающийся агент также будет иметь состояние *Нелояльности*.

Наконец, выделим отказы в отдельное состояние. Представляется очевидным, что конечные паттерны описания отказа в самом агенте не будут зависеть от внешних или внутренних причин. Также можно положить, что паттерны описания отказов среди окружающих агентов будут независимы от внешних или внутренних причин этих отказов. Обозначим это состояние как *Безразличное* (*Ur*) – когда агент по тем или иным причинам не может участвовать во взаимодействии.

Приведенное в предыдущем разделе описание функции *Gen(ME)* позволяет считать, что паттерны описания состояний агента могут так или иначе пересекаться, вплоть до полного совпадения для отдельных паттернов. Это связано как с возможностью ошибок при оценке состояния, так и с тем, что все паттерны агента формируются на основе одного и того же множества событий и сообщений *QM*. Соответственно, необходимо ввести еще одно состояние агента *Индифферентное* (*Ir*). Под этим будем понимать ситуацию, когда агент не может различить состояние окружающих его агентов и с целью обеспечения функционирования ИС готов принимать любые действия окружающих агентов, даже связанные с возможным нанесением ему ущерба.

Таким образом, каждый агент на основании доступного ему множества событий и сообщений *QM* принимает определенное состояние для взаимодействия с каждым из окружающих агентов из множества возможных состояний: $R = \{Lr, Dr, Ir, Ur\}$. Учтем, что оценка состояний агентом имеет определенную долю уверенности *P* в силу ошибок первого и второго рода и тогда формальное описание состояния данного агента для отношений с любым из агентов его окружения будет иметь вид

$$r = P(Ref(\bigcup_{i \in QS} \psi_i) \cup (\bigcup_{j \in QR} \psi_j)), r \in R \quad (14)$$

Приведенные рассуждения позволяют положить, что обобщенное состояние агента представляет собой вектор его состояний, определяемых для каждого из агентов окружения. Обозначим множество агентов как *AG*, а подмножество агентов, взаимодействующих с данным – как *AV*. Соответственно, общее состояние агента *Q* с учетом (14) описывается как:

$$Q_a = [r_1, \dots, r_n], n = |AV|, AV \subset AG, \quad a \in AG \wedge a \notin AV \quad (15)$$

Отношения агентов

Выражения (12) и (13) показывают, что состояние агента и его оценки окружения определяются отношениями между ИП и ИР из его состава. В ИБ принято оценивать такие отношения с точки зрения соблюдения конфиденциальности, целостности и доступности. Для агента конфиденциальность полностью определяется аккаунтом, в рамках которого функционируют ИП

и ИР агента. Из требования обеспечения целостности и доступности вытекает необходимость рассматривать отношения между ИП и ИР агента только как Лояльные (Lr), а также симметричные и рефлексивные. Это позволяет сформулировать аксиому лояльности (здесь и далее нумерация аксиом является продолжением нумерации первой части статьи).

Аксиома 7. Лояльность ИП и ИР внутри агента

$$x[Lr]x =: x \in (QR \vee QS),$$
$$x[Lr]y = y[Lr]x : x \in QR, y \in QS,$$
$$a[Lr]b : a, b \in QR, \quad (16)$$
$$a[Lr]b : a, b \in QS,$$

где *QR* – ИП и *QS* – ИР из состава агента.

Полагаем, что отношение Безразличия (Ur) между ИП и ИР соответствует неработоспособности агента. Характеристика Нелояльности или Индифферентности для отношений ИП и ИР агента невозможно в силу того, что в структуре агента отсутствует возможность разделять деятельность субъектов в пределах аккаунта. То есть, для субъекта (Нарушителя или Защитника) целеполагание может быть сведено к получению и использованию прав доступа к ИП и ИР агента. Эти же рассуждения позволяют положить наличие транзитивности в отношениях ИП и ИР агента. Таким образом, при применении логико-вероятностного метода в ИБ можно исключить из рассмотрения отношения ИП и ИР внутри агента в силу их эквивалентности, независимо от их состава (мощности множеств *QR* и *QS*), определяемого аккаунтом агента.

На диаграмме отображения целей субъекта на объект (рисунок 2) отметим следующие морфизмы, сочетание которых показывает, что для достижения своих целей субъект должен манипулировать с конфигурациями узла:

$g6 = g4 \circ g1$ – представляющий выражение (2);

$g4 = g3 \circ g5$ – показывающий, что для достижения целей субъекта необходимо наличие пути доступа к объекту;

$g6 = g3 \circ g2$ – показывающий, что для манипулирования правилами субъекту необходимо наличие пути доступа к объекту.

Таким образом, можем сформулировать следующую аксиому

Аксиома 8. Любой субъект – пользователь ИС представлен в ИС как агент

$$\forall s \in AS \; \exists a \in AG \quad (17)$$

где *AS* – множество субъектов – пользователей и *AG* – множество агентов ИС.

На диаграмме, приведенной на рисунке 3, отметим следующие морфизмы:

$s6 = g3 \circ s4$ – подтверждающий необходимость и достаточность представления аккаунта как отображения субъекта на узле;

$g1 = s5 \circ s1$ – показывающий, что достижение целей субъекта полностью определяются множествами конфигураций и программ узла;

$s3 = p4 \circ s1$ – соответствующий соотношению между конфигурациями, программами и аккаунтом, то есть определяющий права доступа.

Эти морфизмы позволяют рассматривать выражение (10) как описание одного из возможных аккаунтов узла ИС. Но если посмотреть на выражение (10) с точки зрения системного администрирования, то оно будет соответствовать аккаунту системного администратора узла (root, system, superuser и т.п.), которому доступны для выполнения действий все ИП и ИР узла. Эту аналогию можно распространить и на другие уровни современных ИС – виртуализация ИР и ИП позволяет рассматривать их как часть ресурсов соответствующей платформы виртуализации [12]. С учетом рисунка 5, рассуждений при выводе выражений (8) и (9), можно предположить наличие аккаунтов для различных подсистем и типов данных в ИС. То есть, все уровни ИС с точки зрения ИБ могут быть описаны единым образом – с помощью выражения (10) или с помощью понятия агента ИБ (*ISA*). Универсальность понятия агента базируется на едином подходе к описанию различных уровней – от отдельного сервиса (один сервис-один аккаунт-один поток) до ИС целиком – за счет определения подмножеств ИП и ИР включенных в отдельный аккаунт. То есть можем сформулировать аксиому эквивалентности агентов.

Аксиома 9. Для иерархии аккаунтов ИС существует эквивалентная иерархия агентов данной ИС.

$$\forall a \in AG \; \exists c \in AC \mid AG\{a_1, \ldots, a_i, \leq\}, \quad (18)$$
$$\leftrightarrow AC\{c_1, \ldots, c_j, \leq\}$$

где *AG* – множество агентов и *AC* – множество аккаунтов ИС.

На диаграмме отображения субъекта на объект (рисунок 1) отметим следующие морфизмы:

$p9 = p7 \circ p5$ и $p8 = p9 \circ p1$ – соответствующие использованию субъектом программ и данных, то есть определяющие его возможные действия *SA*;

$p2 = p5 \circ p1$ – соответствующий соотношению между данными, программами и аккаунтом, то есть определяющий права доступа;

$p10 = p7 \circ p3 = p9 \circ p4$ – определяющий возможности субъекта по оценке состояния узла в процессе его функционирования.

Эти морфизмы, а также рисунок 6 и выражения (3), (11), (14) показывают, что функционирование агента, выражающее целеполагание субъекта, может быть представлено как: $Gen(ME) \to Ref(ME) \to Sel(SA)$, что соответствует положениям и выводам первой части статьи. Обозначим отношение между агентами как *RA*. Предложенные ранее описание функций *Gen, Ref* как программно реализуемых автоматов позволяют считать, что каждое отношение каждого агента представляет собой выражение: $RA = \{Ref(ME) \circ Gen(ME) \circ Sel(SA)\}$. То есть, с учетом предыдущих аксиом, определим аксиому эквивалентности отношений

Аксиома 10. Отношения «субъект-субъект»(*RS*) и «субъект-объект» (*RO*) в ИС эквивалентны отношениям агентов из состава ИС.

$$(s_i RS s_j \vee sROv) \mid \forall s \in AS\ v \in V \leftrightarrow \exists (a_k RA a_l) \mid \forall a \in AG, \quad (19)$$

где *AS* – множество субъектов – пользователей, *V* – множество узлов (компонент) и *AG* – множество агентов ИС.

На основании выражения (10) агент описывается ИП, ИР и аккаунтом $a[\![QR, QS, ac]\!]$, $a \in AG$, $ac \in AC$. Соответственно, можем определить отношение агентов следующим образом: $xRAy \mid x[\![QR_x, QS_x. ac_x]\!], y[\![QR_y, QS_y, ac_y]\!]$. Прежде всего отметим, что взаимодействующие агенты в большинстве случаев будут иметь разные аккаунты $ac_x \neq ac_v$. Аналогично можно сказать и относительно ИР $QR_x \neq QR_y$. Выражение (11) показывает, что каждый агент, участвующий во взаимодействии, определяет состояние другого участника отношения только на основании событий и сообщений собственных ИР. Тогда по аналогии с первой частью отношения между двумя агентами $\forall (x, y) \in AG$:

$$xRAy = \{Ref^x(ME^x) \circ Gen^x(ME^x) \circ Sel^x(SA^x)\}$$
$$yRAx = \{Ref^y(ME^y) \circ Gen^y(ME^y) \circ Sel^y(SA^y)\}$$

В силу независимости генерации событий и сообщений каждым из агентов – участников отношения действуют аксиомы 1 и 7, что позволяет положить асимметричность отношений агентов $xRAy \neq yRAx$ или $x[R] \neq y[R]$. Для формирования отношения, то есть определения агентом состояния респондента отношения, этот респондент должен воздействовать на агента так, чтобы у агента сформировались события и сообщения. То есть, взаимодействие агентов определяется связями графа ИС $G(V, E)$, что позволяет отождествить ИП агентов со связями графа $E\left[\!\left[x \overset{R}{\to} y \neq y \overset{R}{\to} x\right]\!\right]$. Или иначе – рассматривать ИП как носители отношений (что соответствует положениям теории системного анализа) $xRy \mid (x[\![QR_x, QS_x]\!], y[\![QR_y, QS_y]\!]) \Rightarrow R[\![QS_x, QS_y]\!]$.

Это позволяет ввести аксиому двойственности. Следуя соглашениям, принятым в первой части статьи, формальная запись будет иметь вид:

Аксиома 11. Любая связь в многоагентной ИС или отношение агентов этой ИС описывается (должна быть помечена) двумя значениями состояний отношения

$$G(V, E): E[\![x[R] \wedge y[R]]\!], \quad \forall (x, y) \in AG, x \neq y \quad (20)$$

Поскольку для обеспечения взаимодействия ИП должны быть согласованы, то набор возможных состояний агента в процессе его функционирования и взаимодействия с окружением могут быть представлены единым множеством $R = \{Lr, Dr, Ir, Ur\}$, независимо от типа аккаунта и числа ИП и ИР в составе агента.

В качестве итога на основании (15) определим состояние агента в виде вектора

$$Q_a = [x[R]_1, \dots, x[R]_n], n = |AV|, \quad AV \subset AG, x \in AV, a \in AG, a \neq x \quad (21)$$

Приведенные аксиомы позволяют указать на следующие свойства подобия, позволяющие описывать различные уровни ИС в терминах агентов.

Prop 1, На любом уровне ИС (представляющая собой множество ИП, ИР и аккаунтов) может быть представлена как подмножество ИП и ИР включенных в отдельный аккаунт, то есть как агент ИБ.

Prop 2. Отношения между агентами формируются единым способом – на основе имеющихся в его распоряжении события и сообщений.

Prop 3. Отношения агентов описываются единообразным набором состояний не зависимо от того, какой уровень описывает агент ИБ.

Prop 4. Состояние агента определяется вектором состояний его окружения не зависимо от того, какой уровень описывает агент ИБ.

Таким образом, агент ИБ обладает свойством самоподобия с точки зрения ИБ и любая ИС может быть представлена в виде вложенных структур, состоящих из ИР, ИП и аккаунтов, то есть агент является универсальной структурой.

Заключение

Для достижения общей цели исследования (адаптации логико-вероятностного метода для решения задач ИБ) в статье разработаны формально-логические основы для определения и последующего выделения фрактальных структур, присущих ИС как сложной системе. Предложено выделить в ИС макроуровень в виде агентов информационной безопасности, состоящих из информационных ресурсов, информационных потоков и прав доступа аккаунта субъекта. Проведен анализ отношений между агентами с использованием аппарата математических и логических отношений. В качестве основных результатов настоящего исследования отметим следующее.

1. Целесообразно в дальнейшем рассматривать с точки зрения ИБ любую ИС, обычно представляемую в виде графа *G(V,E),* как многоагентную систему.

2. Определение агента как обладающего ограниченными свойствами рациональности и интеллектуальности, а также свойства подобия позволяют перенести рассмотрение отношений «субъект-субъект» и «субъект-объект» в ИБ на уровень отношений между агентами.

3. Агент может определять действия субъектов (других агентов) только за счет ИП со своим окружением и/или внешней информации из других источников.

4. Отношения агентов является местом формирования и разрешения конфликта, вызванного отношениями субъектов.

5. Рассмотрение отношений ИП и ИР внутри агента можно исключить из дальнейшего анализа.

6. Объективно в структуре агента отсутствует возможность разделять деятельность субъектов в пределах одного аккаунта, то есть каждый агент и ИС в целом индифферентны к целеполаганию субъектов.

7. С точки зрения ИБ отношение агентов может быть представлено как попарное взаимодействие агентов, определяемое соответствующими состояниями этих агентов.

Литература

1. Рябинин И. А. Решение одной задачи оценки надежности структурно-сложной системы разными логико-вероятностными методами / И.А. Рябинин, А.В. Струков // Моделирование и анализ безопасности и риска в сложных системах, Санкт-Петербург, 19–21 июня 2019 года. – Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2019. – С. 159-172.
2. Демин А. В. Глубокое обучение адаптивных систем управления на основе логико-вероятностного подхода / А.В. Демин // Известия Иркутского государственного университета. Серия: Математика. – 2021. – Т. 38. – С. 65-83. – DOI 10.26516/1997-7670.2021.38.65
3. Викторова В.С. Вычисление показателей надежности в немонотонных логико-вероятностных моделях многоуровневых систем / В.С. Викторова, А.С. Степанянц // Автоматика и телемеханика. – 2021. – № 5. – С. 106-123. – DOI 10.31857/S000523102105007X.
4. Леонтьев А.С. Математические модели оценки показателей надежности для исследования вероятностно-временных характеристик многомашинных комплексов с учетом отказов / А.С. Леонтьев, М.С. Тимошкин // Международный научно-исследовательский журнал. – 2023. – № 1(127). С. 1 – 13. – DOI 10.23670/IRJ.2023.127.27.
5. Пучкова Ф.Ю. Логико-вероятностный метод и его практическое использование / Ф.Ю. Пучкова // Информационные технологии в процессе подготовки современного специалиста: Межвузовский сборник научных трудов / Министерство просвещения Российской Федерации; Федеральное государственное бюджетное образовательное учреждение высшего образования «Липецкий государственный педагогический университет имени П.П. СЕМЕНОВА-ТЯН-ШАНСКОГО». Том Выпуск 25. – Липецк: Липецкий государственный педагогический университет имени П.П. Семенова-Тян-Шанского, 2021. – С. 187-193.
6. Россихина Л.В. О применении логико-вероятностного метода И.А. Рябинина для анализа рисков информационной безопасности / Л.В. Россихина, О.О. Губенко, М.А. Черноситова // Актуальные проблемы деятельности подразделений УИС: Сборник материалов Всероссийской научно-практической конференции, Воронеж, 20 октября 2022 года. – Воронеж: Издательско-полиграфический центр «Научная книга», 2022. – С. 108-109.
7. Карпов А.В. Модель канала утечки информации на объекте информатизации / А.В. Карпов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах, Санкт-Петербург, 28 февраля – 01 марта 2018 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2018. – С. 378-382.
8. Методика кибернетической устойчивости в условиях воздействия таргетированных кибернетических атак / Д.А. Иванов, М.А. Коцыняк, О.С. Лаута, И.Р. Муртазин // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах, Санкт-Петербург, 28 февраля – 01 марта 2018 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2018. – С. 343-346.

9. Елисеев Н. И. Оценка уровня защищенности автоматизированных информационных систем юридически значимого электронного документооборота на основе логико-вероятностного метода / Н.И. Елисеев, Д.И. Тали, А.А. Обланенко // Вопросы кибербезопасности. – 2019. – № 6(34). – С. 7-16. – DOI 10.21681/2311-3456-2019-6-07-16.
10. Коцыняк М.А. Математическая модель таргетированной компьютерной атаки / М.А. Коцыняк, О.С. Лаута, Д.А. Иванов // Наукоемкие технологии в космических исследованиях Земли. – 2019. – Т. 11, № 2. – С. 73-81. – DOI 10.24411/2409-5419-2018-10261.
11. Белякова Т.В. Функциональная модель процесса воздействия целевой компьютерной атаки / Т.В. Белякова, Н.В. Сидоров, М.А. Гудков // Радиолокация, навигация, связь: Сборник трудов XXV Международной научно-технической конференции, посвященной 160-летию со дня рождения А.С. Попова. В 6-ти томах, Воронеж, 16–18 апреля 2019 года. Том 2. – Воронеж: Воронежский государственный университет, 2019. – С. 108-111.
12. Калашников А. О. Инфраструктура как код: формируется новая реальность информационной безопасности / А.О. Калашников, К.А. Бугайский // Информация и безопасность. – 2019. – Т. 22, № 4. – С. 495-506.
13. Бугайский К.А. Расширенная модель открытых систем (Часть 1) / К. А. Бугайский, Д. С. Бирин, Б. О. Дерябин, С. О. Цепенда // Информация и безопасность. – 2022. – Т. 25, № 2. – С. 169-178. – DOI 10.36622/VSTU.2022.25.2.001.
14. Нестеров А. Ю. Проблема субъекта в искусственной природе / А. Ю. Нестеров // Гуманитарный вектор. – 2021. – Т. 16, № 2. – С. 22-28. – DOI 10.21209/1996-7853-2021-16-2-22-28.
15. Дыдров А. А. Построение дискурса о цифровом как феномене информационной современности / А. А. Дыдров, Р. В. Пеннер // Социум и власть. – 2022. – № 3(93). – С. 114-126. – DOI 10.22394/1996-0522-2022-3-114-126. .
16. Бугайский К. А. Расширенная модель открытых систем (Часть 2) / К.А. Бугайский, И.С. Перескоков, А.О. Петров, А.О. Петров // Информация и безопасность. – 2022. – Т. 25, № 3. – С. 321-330. – DOI 10.36622/VSTU.2022.25.3.001.
17. Бугайский К. А. Расширенная модель открытых систем (Часть 3) / К.А. Бугайский, Б.О. Дерябин, К.В. Табаков, Е.С. Храмченкова, С.О. Цепенда // Информация и безопасность. – 2022. – Т. 25, № 4. – С. 501-512.
18. Калашников А. О. Модель количественного оценивания агента сложной сети в условиях неполной информированности / А. О. Калашников, К. А. Бугайский // Вопросы кибербезопасности. – 2021. – № 6(46). – С. 26-35. – DOI 10.21681/2311-3456-2021-6-26-35.
19. Максимов Д. Ю. Формирование оптимального маршрута в конфигурационном пространстве больших групп интеллектуальных агентов с помощью линейной логики / Д. Ю. Максимов // Управление развитием крупномасштабных систем (MLSD'2018) : Материалы одиннадцатой международной конференции. В 2-х томах, Москва, 01–03 октября 2018 года / Под общей редакцией С.Н. Васильева, А.Д. Цвиркуна. Том I. – Москва: Институт проблем управления им. В.А. Трапезникова РАН, 2018. – С. 309-311.
20. Левкина И. Н. Общая структура многоагентной системы поддержки принятия решений shape * MERGEFORMAT / И. Н. Левкина, Т. М. Леденева // Евразийский союз ученых. – 2020. – № 5-5(74). – С. 43–46.
21. Применение логико-вероятностного метода в информационной безопасности (Часть 2) / Калашников А.О., Бугайский К.А., Бирин Д.С., Дерябин Б.О., Цепенда С.О., Табаков К.В. // Вопросы кибербезопасности. – 2023. – № 4(56). – С. 23–32. – DOI 10.21681/2311-3456-2023-4-23-32.

APPLICATION OF THE LOGICAL-PROBABILISTIC METHOD IN INFORMATION SECURITY (PART 1)

Kalashnikov A.O.[9], Bugajskij K.A.[10], Anikina E.V.[11], Pereskokov I.S.[12], Petrov Andrej O.[13], Petrov AleksandrO.[14], Hramchenkova E.S.[15], Molotov A.A.[16]

The purpose of the article: *adaptation of the logical-probabilistic method of evaluating complex systems to the tasks of building information security systems in a multi-agent system.*

Research method: *during the research, the main provisions of the methodology of structural analysis, system analysis, decision theory, methods of evaluating events under the condition of incomplete information were used.*

The result: *this article continues the consideration of information security issues based on the analysis of the relationship between the subjects and the object of protection. The presentation of the subject and object*

[9] Andrey Kalashnikov, Dr.Sc., Chief Scientist of the Laboratory «Complex networks» Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: aokalash@ipu.ru

[10] Konstantin Bugajskij, Junior Researcher of the Laboratory «Complex networks» Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E mail: kabuga@ipu.ru

[11] Eugenia Anikina – research fellow, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, e-mail: ajanet@ipu.ru

[12] Ilia Pereskokov – junior researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, e-mail: pereskokov @phystech.edu

[13] Andrei Petrov – junior researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, e-mail: petrovaojob@gmail.com

[14] Aleksandr Petrov – junior researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, e-mail: petrovalexandr@ipu.ru

[15] Ekaterina Hramchenkova– junior researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, e-mail: hramchenkovaes@yandex.ru

[16] Aleksandr Molotov, software engineer Institute of Control Sciences of Russian Academy of Sciences. E mail: alpha.sphere@ya.ru

of protection in the form of an intelligent agent is justified, taking into account the requirements for information protection. Formal definitions of the information security agent and its main characteristics are given: information resource, information flow and access rights of the subject. It is shown that the concept of an information security agent is the basis for identifying structures in an information system. The axiomatics of the relations of the subject and the object as agents of information security, as well as the relations between information resources and information flows within the agent, has been developed. The possibility of determining the state of an agent based on events and messages generated during its operation is shown.

Scientific novelty: *consideration of information security issues using the apparatus of mathematical and logical relations. Development of formal definitions of the information security agent and its constituent information resources and information flows, which are the basic universal components of the description of structures in the information system. Definition of the concept of an information security agent by considering the mapping of the subject and its goal-setting on the object..*

Keywords: *information security model, assessment of complex systems, logical-probabilistic method, theory of relations, system analysis, multi-agent system.*

References

1. Rjabinin I. A. Reshenie odnoj zadachi ocenki nadezhnosti strukturno-slozhnoj sistemy raznymi logiko-verojatnostnymi metodami / I.A. Rjabinin, A.V. Strukov // Modelirovanie i analiz bezopasnosti i riska v slozhnyh sistemah, Sankt-Peterburg, 19–21 ijunja 2019 goda. – Sankt-Peterburg: Sankt-Peterburgskij gosudarstvennyj universitet ajerokosmicheskogo priborostroenija, 2019. – S. 159-172.
2. Demin A. V. Glubokoe obuchenie adaptivnyh sistem upravlenija na osnove logiko-verojatnostnogo podhoda / A.V. Demin // Izvestija Irkutskogo gosudarstvennogo universiteta. Serija: Matematika. – 2021. – T. 38. – S. 65-83. – DOI 10.26516/1997-7670.2021.38.65
3. Viktorova V.S. Vychislenie pokazatelej nadezhnosti v nemonotonnyh logiko-verojatnostnyh modeljah mnogourovnevyh sistem / V.S. Viktorova, A.S. Stepanjanc // Avtomatika i telemehanika. – 2021. – № 5. – S. 106-123. – DOI 10.31857/S000523102105007X.
4. Leont'ev A.S. Matematicheskie modeli ocenki pokazatelej nadezhnosti dlja issledovanija verojatnostno-vremennyh harakteristik mnogomashinnyh kompleksov s uchetom otkazov / A.S. Leont'ev, M.S. Timoshkin // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal. – 2023. – № 1(127). S. 1 – 13. – DOI 10.23670/IRJ.2023.127.27.
5. Puchkova F.Ju. Logiko-verojatnostnyj metod i ego prakticheskoe ispol'zovanie / F.Ju. Puchkova // Informacionnye tehnologii v processe podgotovki sovremennogo specialista: Mezhvuzovskij sbornik nauchnyh trudov / Ministerstvo prosveshhenija Rossijskoj Federacii; Federal'noe gosudarstvennoe bjudzhetnoe obrazovatel'noe uchrezhdenie vysshego obrazovanija «Lipeckij gosudarstvennyj pedagogicheskij universitet imeni P.P. SEMENOVA-TJaN-ShANSKOGO». Tom Vypusk 25. – Lipeck: Lipeckij gosudarstvennyj pedagogicheskij universitet imeni P.P. Semenova-Tjan-Shanskogo, 2021. – S. 187-193.
6. Rossihina L.V. O primenenii logiko-verojatnostnogo metoda I.A. Rjabinina dlja analiza riskov informacionnoj bezopasnosti / L.V. Rossihina, O.O. Gubenko, M.A. Chernositova // Aktual'nye problemy dejatel'nosti podrazdelenij UIS: Sbornik materialov Vserossijskoj nauchno-prakticheskoj konferencii, Voronezh, 20 oktjabrja 2022 goda. – Voronezh: Izdatel'sko-poligraficheskij centr "Nauchnaja kniga", 2022. – S. 108-109.
7. Karpov A.V. Model' kanala utechki informacii na ob#ekte informatizacii / A.V. Karpov // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO 2018): VII Mezhdunarodnaja nauchno-tehnicheskaja i nauchno-metodicheskaja konferencija. Sbornik nauchnyh statej. V 4-h tomah, Sankt-Peterburg, 28 fevralja – 01 marta 2018 goda / Pod redakciej S.V. Bachevskogo. Tom 2. – Sankt-Peterburg: Sankt-Peterburgskij gosudarstvennyj universitet telekommunikacij im. prof. M.A. Bonch-Bruevicha, 2018. – S. 378-382.
8. Metodika kiberneticheskoj ustojchivosti v uslovijah vozdejstvija targetirovannyh kiberneticheskih atak / D.A. Ivanov, M.A. Kocynjak, O.S. Lauta, I.R. Murtazin // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO 2018): VII Mezhdunarodnaja nauchno-tehnicheskaja i nauchno-metodicheskaja konferencija. Sbornik nauchnyh statej. V 4-h tomah, Sankt-Peterburg, 28 fevralja – 01 marta 2018 goda / Pod redakciej S.V. Bachevskogo. Tom 2. – Sankt-Peterburg: Sankt-Peterburgskij gosudarstvennyj universitet telekommunikacij im. prof. M.A. Bonch-Bruevicha, 2018. – S. 343-346.
9. Eliseev N. I. Ocenka urovnja zashhishhennosti avtomatizirovannyh informacionnyh sistem juridicheski znachimogo jelektronnogo dokumentooborota na osnove logiko-verojatnostnogo metoda / N.I. Eliseev, D.I. Tali, A.A. Oblanenko // Voprosy kiberbezopasnosti. – 2019. – № 6(34). – S. 7-16. – DOI: 10.21681/2311-3456-2019-6-07-16.
10. Kocynjak M.A. Matematicheskaja model' targetirovannoj komp'juternoj ataki / M.A. Kocynjak, O.S. Lauta, D.A. Ivanov // Naukoemkie tehnologii v kosmicheskih issledovanijah Zemli. – 2019. – T. 11, № 2. – S. 73-81. – DOI 10.24411/2409-5419-2018-10261.
11. Beljakova T.V. Funkcional'naja model' processa vozdejstvija celevoj komp'juternoj ataki / T.V. Beljakova, N.V. Sidorov, M.A. Gudkov // Radiolokacija, navigacija, svjaz': Sbornik trudov XXV Mezhdunarodnoj nauchno-tehnicheskoj konferencii, posvjashhennoj 160-letiju so dnja rozhdenija A.S. Popova. V 6-ti tomah, Voronezh, 16–18 aprelja 2019 goda. Tom 2. – Voronezh: Voronezhskij gosudarstvennyj universitet, 2019. – S. 108-111.
12. Kalashnikov A. O. Infrastruktura kak kod: formiruetsja novaja real'nost' informacionnoj bezopasnosti / A.O. Kalashnikov, K.A. Bugajskij // Informacija i bezopasnost'. – 2019. – T. 22, № 4. – S. 495-506.
13. Bugajskij K.A. Rasshirennaja model' otkrytyh sistem (Chast' 1) / K. A. Bugajskij, D. S. Birin, B. O. Derjabin, S. O. Cependa // Informacija i bezopasnost'. – 2022. – T. 25, № 2. – S. 169-178. – DOI 10.36622/VSTU.2022.25.2.001.
14. Nesterov A. Ju. Problema sub#ekta v iskusstvennoj prirode / A. Ju. Nesterov // Gumanitarnyj vektor. – 2021. – T. 16, № 2. – S. 22-28. – DOI 10.21209/1996-7853-2021-16-2-22-28.

15. Dydrov A. A. Postroenie diskursa o cifrovom kak fenomene informacionnoj sovremennosti / A. A. Dydrov, R. V. Penner // Socium i vlast'. – 2022. – № 3(93). – S. 114-126. – DOI 10.22394/1996-0522-2022-3-114-126. .
16. Bugajskij K. A. Rasshirennaja model' otkrytyh sistem (Chast' 2) / K.A. Bugajskij, I.S. Pereskokov, A.O. Petrov, A.O. Petrov // Informacija i bezopasnost'. – 2022. – T. 25, № 3. – S. 321-330. – DOI 10.36622/VSTU.2022.25.3.001.
17. Bugajskij K. A. Rasshirennaja model' otkrytyh sistem (Chast' 3) / K.A. Bugajskij, B.O. Derjabin, K.V. Tabakov, E.S. Hramchenkova, S.O. Cependa // Informacija i bezopasnost'. – 2022. – T. 25, № 4. – S. 501-512.
18. Kalashnikov A. O. Model' kolichestvennogo ocenivanija agenta slozhnoj seti v uslovijah nepolnoj informirovannosti / A. O. Kalashnikov, K. A. Bugajskij // Voprosy kiberbezopasnosti. – 2021. – № 6(46). – S. 26-35. – DOI 10.21681/2311-3456-2021-6-26-35.
19. Maksimov D. Ju. Formirovanie optimal'nogo marshruta v konfiguracionnom prostranstve bol'shih grupp intellektual'nyh agentov s pomoshh'ju linejnoj logiki / D. Ju. Maksimov // Upravlenie razvitiem krupnomasshtabnyh sistem (MLSD'2018) : Materialy odinnadcatoj mezhdunarodnoj konferencii. V 2-h tomah, Moskva, 01–03 oktjabrja 2018 goda / Pod obshhej redakciej S.N. Vasil'eva, A.D. Cvirkuna. Tom I. – Moskva: Institut problem upravlenija im. V.A. Trapeznikova RAN, 2018. – S. 309-311.
20. Levkina I. N. Obshhaja struktura mnogoagentnoj sistemy podderzhki prinjatija reshenij shape * MERGEFORMAT / I. N. Levkina, T. M. Ledeneva // Evrazijskij sojuz uchenyh. – 2020. – № 5-5(74). – S. 43–46.
21. Primenenie logiko-verojatnostnogo metoda v informacionnoj bezopasnosti (Chast' 2) / Kalashnikov A.O., Bugajskij K.A., Birin D.S., Derjabin B.O., Cependa S.O., Tabakov K.V. // Voprosy kiberbezopasnosti. – 2023. – № 4(56). – S. 23–32. – DOI 10.21681/2311-3456-2023-4-23-32.