ПРИМЕНЕНИЕ ЛОГИКО-ВЕРОЯТНОСТНОГО МЕТОДА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ЧАСТЬ 1)

Калашников А.О.[1], Бугайский К.А.[2], Бирин Д.С.[3], Дерябин Б.О.[4], Цепенда С.О. [5], Табаков К.В.[6]

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: *в данной статье предложено рассматривать вопросы информационной безопасности на основе анализа отношений между субъектами и объектом защиты. Определены типы отношений «субъект-субъект», «субъект-объект» и приведена базовая аксиоматика отношений с учетом требований по защите информации. На основе аксиоматики даны формальные логические определения основных элементов информационной безопасности: нарушитель, защитник, пользователь, внутренний нарушитель, атака, защита, противоборство. По результатам анализа отношений показано, что нарушитель и защитник используют единый источник информации для принятия решений, но при этом их деятельность по оценке ситуации и выбору действий носит асимметричный характер. Проведенный анализ отношений позволил дать формальное логическое описание процессов взаимодействия субъектов между собой и с объектом защиты. Что представляет собой основу для выделения фрактальных структур в информационной системе.*

Научная новизна: *рассмотрение вопросов защиты информации с использованием аппарата математических и логических отношений. Разработка формальных логических выражений, описывающих взаимодействие нарушителя и защитника между собой, а также с объектом защиты.*

Вклад авторов: *Калашников А.О. выполнил постановку задачи и общую разработку модели применения логико-вероятностного метода в информационной безопасности. Бугайский К.А. разработал модель применения и адаптации логико-вероятностного метода в информационной безопасности. Бирин Д.С. и Дерябин Б.О. разработали типы и аксиоматику отношений. Цепенда С.О. и Табаков К.В. разработали определения функций коммутативной диаграммы.*

Ключевые слова: *модель информационной безопасности, оценка сложных систем, логико-вероятностный метод, теория отношений, системный анализ*

DOI:10.21681/2311-3456-2023-4-23-32

Введение

Данная статья является первой из серии публикаций, посвященных исследованию вопроса применения логико-вероятностного метода при изучении вопросов защиты информации. Метод был разработан Рябининым И.А. [1, см. литературу там же]. 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.

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

2 Бугайский Константин Алексеевич, младший научный сотрудник, Институт проблем управления им. В.А. Трапезникова РАН, e-mail: kabuga@ipu.ru

3 Бирин Денис Сергеевич, младший научный сотрудник, Институт проблем управления им. В.А. Трапезникова РАН, e-mail: birin@phystech.edu

4 Дерябин Богдан Олегович, младший научный сотрудник, Институт проблем управления им. В.А. Трапезникова РАН, e-mail: baga_d@mail.ru

5 Цепенда Сергей Олегович, младший научный сотрудник, Институт проблем управления им. В.А. Трапезникова РАН, e-mail: tsepende.s@gmail.com

6 Табаков Кирилл Викторович, младший научный сотрудник, Институт проблем управления им. В.А. Трапезникова РАН, e-mail: tabakov2002@mail.ru

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 предпринята попытка разработать формально-логические основы для определения возможности наличия и последующего выделения фрактальных структур, присущих ИС как сложной системе. Для решения этой задачи выделяется метауровень ИС, состоящий из субъектов и объекта защиты, и проводится рассмотрение отношений между ними.

Субъекты ИБ

Традиционно рассмотрение вопросов ИБ ведется в терминах Защитник, Нарушитель, Информационная система (ИС) и Пользователь ИС. При этом ИС рассматривается как объект защиты, а Защитник, Нарушитель и Пользователь – как субъекты, – как правило, физические лица. Объект защиты будем представлять в виде графа $G(V,E)$ и в дальнейшем использовать термины «узел графа» и «компонент ИС» как синонимы. Субъекты, как правило, обозначаются как «Защитник», «Нарушитель», «Пользователь» и в общем виде представляют из себя множества *D, H, U* соответственно. Образуем из этих множеств множество субъектов $AS=\{D,H,U\}$ такое, что $AS=D\cup H\cup U$ и $D\cap H=\varnothing$, а также примем, без потери общности, что $H\cap U=\varnothing$, $D\cap U=\varnothing$. На данном этапе не будем учитывать внутреннюю структуру множеств *D, H, U*, а рассмотрим взаимодействие субъектов между собой, а также с ИС – как единым объектом.

В качестве основных характеристик субъекта выделим:

— целеполагание (goal setting – *GS*);
— набор действий (set of actions – *SA*);
— уровень квалификации (qualification level – *QL*);
— доступные ресурсы (available resources – *AR*).

Будем полагать, что для целей исследования все субъекты множества *AS* в достаточной мере описываются этими характеристиками: $AS[\![GS,SA,QL,AR]\!]$. Рассматривая целеполагание как волевой акт субъекта отметим следующее.

1. Для Пользователя цели его деятельности находятся вне ИС, которая рассматривается им только как инструмент, обеспечивающий определенные этапы достижения целей, связанных с обработкой информации, то есть $u[\![GS=\varnothing]\!]$, $u\in U$.

2. Для Нарушителя достижение цели (как правило она связана с обогащением) полностью определяется его деятельностью в рамках ИС. Поскольку в ИБ цели Нарушителя определяются как «нарушение конфиденциальности, целостности и доступности» компонент ИС и обрабатываемой в ней информации, то целесообразно ограничить целеполагание Нарушителя пределами ИС. То есть $GS[\![G(V,E)]\!]$ и

$$h[\![GS,SA,QL,AR]\!]\Rightarrow[\![GSG(V,E)]\!],\ h\in H \qquad (1).$$

3. Для Защитника цели полностью определяются заданными параметрами функционирования ИС, то есть его целеполагание так же ограничивается пределами ИС. В соответствии с нормативными документами по защите информации целесообразно положить, что целеполагание Защитника прямо противоположно целеполаганию Нарушителя. То есть $\neg GS[\![G(V,E)]\!]$ или $\overline{GS}[\![G(V,E)]\!]$ и

$d[\![GS,SA,QL,AR]\!] \Rightarrow [\![\overline{GS}G(V,E)]\!],\ d \in D$ (2).

Выражения (1) и (2) представляют собой высказывания, описывающие взаимодействие Нарушителя и Защитника с объектом, который обозначим как $S = G(V,E)$. В силу $GS[\![G(V,E)]\!]$ и $\overline{GS}[\![G(V,E)]\!]$ взаимодействие непосредственно между Нарушителем и Защитником целесообразно рассматривать опосредованно – через ИС, что дает отношения $D \times H$, $D \times S$ и $H \times S$. Применительно к Пользователю имеем отношения $D \times U$, $H \times U$ и $U \times S$. Пользователя, как правило, не будем учитывать (см. п.1 выше) во взаимодействиях субъектов из множества *AS* и объекта.

Взаимодействие между субъектами и объектом можно определить как функцию, аргументами которой являются элементы множеств и тогда отношения между ними можно представить как предикат в виде xRy.

Для различения взаимодействий между субъектами и между субъектами и объектом введем типы отношений:

$$RS:(\forall x \in H \wedge \forall y \in D) \vee (\forall x \in D \wedge \forall y \in H) \vee (\forall x \in U \wedge \forall y \in H,D) \vee (\forall x \in H,D \wedge \forall y \in U)$$

– для обозначения взаимодействия субъектов между собой;

$$RO:(\forall x \in H,D,U) \wedge (\forall y \in S) \vee (\forall x \in S) \wedge (\forall y \in H,D,U)$$

– для обозначения взаимодействия субъектов и объекта.

Таким образом, например, отношения Защитник и Нарушитель примут вид *dRSh* или *hRSd*, а отношения пользователя с объектом – *uROs* или *sROu*.

Определим результат вычисления функции xRy применительно к ИБ. Отношение может быть:

Лояльное (*Lr*) – когда участник осуществляет корректное, благожелательное сотрудничество, подразумевающее отсутствие намерений по нанесению ущерба респонденту или объекту.

Нелояльное (*Dr*) – когда действия участника подразумевают нанесение ущерба респонденту, прежде всего за счет нанесения ущерба объекту.

Индифферентное (*Ir*) – когда участник готов принимать любые действия респондента, даже связанные с возможным ущербом.

Безразличное (*Ur*) – когда участник умышленно избегает взаимодействия с респондентом.

Обозначим эти значения как множество $R = \{Lr, Dr, Ir, Ur\}$.

Поскольку предикаты можно рассматривать как функцию, сделаем следующее предположение относительно области значений из *R* для отношений *RS* и *RO*. С одной стороны, ИБ необходимо рассматривать как процесс, то есть в ходе взаимодействия субъектов

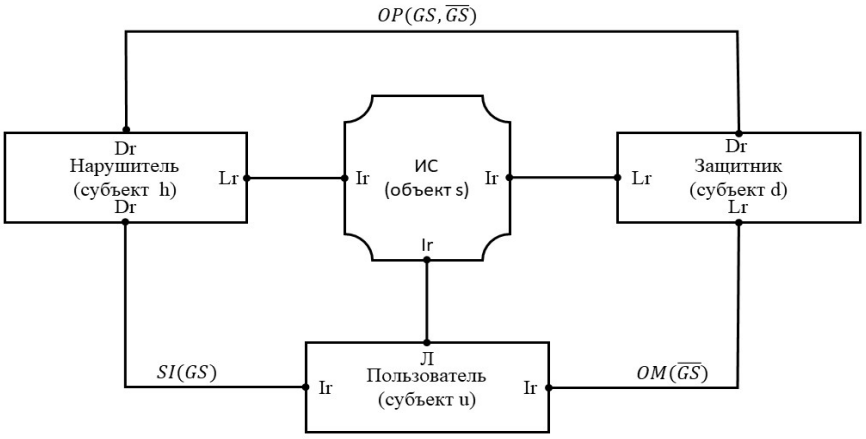

Рис. 1. Схема базовой конфигурации отношений

и объекта, значения отношений *RS* и *RO* из *R* должны изменяться по шагам реализации процесса. С другой стороны, можно определить базовую конфигурацию отношений *RS* и *RO* следующим образом. Схема базовой конфигурации отношений представлена на рисунке 1.

На основании (1) и (2) можно говорить об антагонизме Защитника и Нарушителя, что соответствует Нелояльному отношению друг к другу $dRSh = hRSd = Dr$.

В ИБ принято, что деятельность Нарушителя наносит ущерб пользователю, следовательно, также имеем Нелояльное отношение $hRSu = Dr$.

Отношение Пользователя к Нарушителю можно определить скорее как Лояльное (например, реакция на фишинг) до тех пор, пока действия Нарушителя не влияют на действия Пользователя и оно (возможно) станет Нелояльным. То есть это отношение целесообразно определить как Индифферентное $uRSh = Ir$.

Отношения Пользователя и Защитника можно определить как Лояльное со стороны Защитника $dRSu = Lr$ и Индифферентное со стороны Пользователя $uRSd = Ir$.

Если принять во внимание, что ИС должна обеспечивать свое функционирование в интересах Пользователя даже при условии его некорректных действий, то отношение объекта к субъектам определим на как Индифферентное $sROd = sROh = sROu = Ir$.

Пользователь и Защитник заинтересованы в нормальном функционировании ИС и их отношение к ИС определим как Лояльное $dROs = uROs = Lr$.

Нарушитель заинтересован в доступности элементов ИС для осуществления своих действий. Сохранение доступности так же определяется стремлением Нарушителя обеспечить скрытность своих действий, как минимум, до определенного этапа. Иначе это можно рассматривать как сохранение целостности конфигураций узлов ИС и ИС в целом для обеспечения манипулирования с данными. При этом в отдельных случаях Нарушитель может модифицировать конфигурации для получения доступа к данным, но с сохранением доступности узла. Таким образом можно говорить о том, что в принципе несанкционированный доступ к данным (и конфигурациям) со стороны Нарушителя базируется на сотрудничестве Нарушителя и ИС. Что позволяет положить Лояльным отношение Нарушителя к ИС $hROs = Lr$.

Перечисленные предикаты являются базовыми. Поскольку взаимодействие субъектов в большинстве случаев происходит опосредованно – через ИС, то необходимо ввести дополнительные предикаты.

Ранее было предложено считать, что цели Пользователя находятся вне ИС и он Индифферентен по отношению к Нарушителю и Защитнику. Следовательно, можно положить, что Пользователь подвергается воздействию:

- со стороны Нарушителя, что можно рассматривать как социальную инженерию в широком смысле, которая может осуществляться непосредственно или через объект $SI(GS) = (hRSu \wedge uRSh) \vee (hROs \wedge uROs)$;
- со стороны Защитника, что можно трактовать как организационно-технические мероприятия, которые могут осуществляться непосредственно или через объект $OM(\overline{GS}) = (dRSu \wedge uRSd) \vee (dROs \wedge uROs)$.

Набор действий Пользователя полностью определяется перечнем узлов ИС и функций на них, доступ к которым предоставлен Защитником. Однако Пользователь может в силу разных причин выйти (пытаться выйти) за пределы предоставленных ему возможностей $SI(GS) > OM(\overline{GS})$, то есть изменить отношение на Нелояльное $uRSd = Dr$. В этом случае целесообразно рассматривать Пользователя в качестве Нарушителя (внутренний нарушитель). При этом отношение $uROs = Lr$ останется неизменным.

Взаимодействие Защитника и Нарушителя непосредственно осуществляется на объекте, но нельзя исключать и возможное воздействие Нарушителя непосредственно на Защитника (подкуп, шантаж) $OP(GS, \overline{GS}) = (dROs \wedge hROs) \vee hRSd$.

Аксиоматика отношений субъектов

Приведенные определения области значений предикатов позволяют утверждать, что отношение из *RS* или *RO* имеет направление «слева направо». Для упрощения формы записей отношений будем обозначать отношение как $x \overset{R}{\rightarrow} y$ с указанием принадлежности респондентов множествам *AS* или *S*, а также с указанием в квадратных скобках значения отношений из *R* для данного респондента $x[r]$, $r \in R$.

Аксиома 1. Асимметричности отношений, при любых их значениях:

$$\forall (x, y) : (x[R] \wedge y[R]) \Rightarrow \left(x \overset{R}{\rightarrow} y \neq y \overset{R}{\rightarrow} x \right)$$

Аксиома 2. Однозначности отношений Защитника и Нарушителя, которые могут иметь только Нелояльные отношения друг с другом:

$$x \overset{R}{\rightarrow} y : (x \in H \wedge y \in D) \vee$$

$$\vee (x \in D \wedge y \in H) \Rightarrow !\exists \left((x[Dr]) \wedge (y[Dr]) \right)$$

Аксиома 3. Ограниченной рефлексии. Респондент отношения может быть только Лояльным или Безразличным (отключенным) по отношению к себе:

$$x \xrightarrow{R} x : \left(x\left[Lr \wedge \overline{Dr} \wedge \overline{Ir} \wedge \overline{Ur}\right]\right) \vee \vee \left(x\left[Ur \wedge \overline{Lr} \wedge \overline{Dr} \wedge \overline{Ir}\right]\right)$$

Аксиома 4. Отсутствия отношений. Если один или оба респондента отношения имеют значение Безразличие, то это отношение не существует:

$$\forall (x,y) : \left(x[Ur]\right) \vee \left(y[Ur]\right) \Rightarrow \neg\left(x \xrightarrow{R} y\right)$$

Аксиома 5. Единственности для респондента значения из *R* в фиксированный момент времени:

$$\forall (x,y) : (x \wedge y) \bigtimes \bigtimes \left[Lr\overline{Dr}\,\overline{Ir}\overline{Ur} \vee \overline{Lr}Dr\,\overline{Ir}\overline{Ur} \vee \overline{Lr}\,\overline{Dr}Ir\overline{Ur} \vee \overline{Lr}\,\overline{Dr}\,\overline{Ir}Ur\right]$$

Отдельно рассмотрим вопрос транзитивности отношений. В силу того, что взаимодействие субъектов так или иначе осуществляется посредством ИС, то транзитивность имеет место только для последовательности «субъект – объект – субъект» и это единственный случай транзитивности отношений в рассматриваемой схеме взаимоотношений субъектов и объекта.

Аксиома 6. Единственности транзитивности:

$$\left((x,z) \in AS \wedge y \in S \wedge (x,y,z) : [R \setminus Ur]\right) \wedge \wedge \left(x \xrightarrow{R} y, y \xrightarrow{R} z\right) \Rightarrow x \xrightarrow{R} z$$

В качестве промежуточного вывода укажем, что отношения *RS* и *RO* асимметричны, а также ограниченно рефлексивны и ограниченно транзитивны.

Отметим, что Аксиомы 3 – 5 позволяют сузить область определения предикатов до трех значений: Лояльно (*Lr*), Нелояльно (*Dr*) и Индифферентно (*Ir*). В рамках логико-вероятностного подхода дадим определения основных терминов ИБ через логические операции определяющие отношения *RS* или *RO*.

Определение 1. Определение внутреннего нарушителя:

$$\exists x \xrightarrow{R} y : x \in U \wedge \wedge \left(x[Dr]\right) \wedge y \in (D,S,U) \wedge \left(y[R \setminus Ur]\right) \Rightarrow x \in H$$

Определение 2. Описание возможностей Нарушителя:

$$\exists x \xrightarrow{R} y : x \in H \wedge \left(x[R \setminus Ur]\right) \Rightarrow \Rightarrow y \in (U,S) \wedge \left(y[R \setminus Ur]\right)$$

Определение 3. Описание возможностей Защитника:

$$\exists x \xrightarrow{R} y : x \in D \wedge \left(x[R \setminus Ur]\right) \Rightarrow \Rightarrow y \in (U,S) \wedge \left(y[R \setminus Ur]\right)$$

Определение 4. Описание возможностей Пользователя:

$$\exists x \xrightarrow{R} y : x \in U \wedge \left(x[R \setminus Ur]\right) \Rightarrow \Rightarrow y \in (H,D,S) \wedge \left(y[R \setminus Ur]\right)$$

Определение 5. Описание возможностей объекта отношений:

$$\exists x \xrightarrow{R} y : x \in S \wedge \left(x[R \setminus Ur]\right) \Rightarrow \Rightarrow y \in (H,D,U,S) \wedge \left(y[R \setminus Ur]\right)$$

Определение 6. Определение атаки

$$\exists x \xrightarrow{R} y : x \in H \wedge y \in (D,U,S) \wedge \left(x[Dr] \wedge y[Lr,Ir]\right)$$

Определение 7. Определение защиты

$$\exists x \xrightarrow{R} y : x \in D \wedge y \in (H,U,S) \wedge x[Dr] \wedge y[Lr,Ir])$$

Определение 8. Определение противоборства/конфликта

$$\exists x \xrightarrow{R} y : x \in H \wedge y \in (D,U,S) \wedge \left(x[Dr] \wedge y[Dr]\right)$$

Дополнительные аксиомы и определения, связанные с отношениями узлов ИС, а также определяющие операции с отношениями будут приведены позднее.

Область определения отношений субъектов

В самом общем виде область определения для отношений субъектов может быть описана через уровень квалификации *QL* субъекта и доступные ему ресурсы *AR*. Оба этих качества могут быть описаны как способность субъекта выполнять определенные действия по достижению целей на основании получаемой информации о составе ИС, связях между компонентами ИС $G(V,E)$, характеристиками этих компонент $V[\![Res]\!]$. Под характеристиками узлов ИС будем понимать [14, 15] перечень данных, реализуемых алгоритмов (программ) и обеспечивающих их конфигураций $Res = \{Data, Prog, Conf\}$. В свою очередь, алгоритмы и их конфигурации с точки зрения ИБ описываются «слабостями» (в терминах MITRE) – *WE*.

То есть, имеем $(QL, AR)[\![G(V,E), Res, WE]\!]$. Тогда можно положить, что для Нарушителя и Защитника

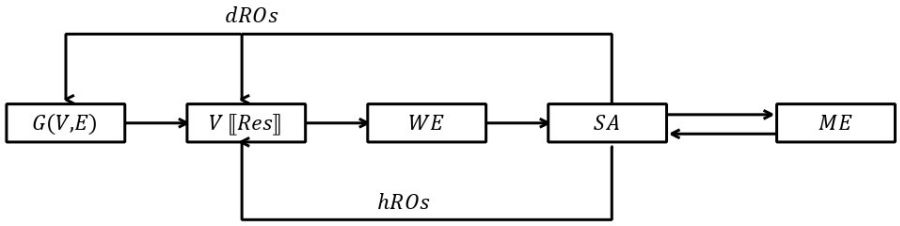

Рис. 2. Схема импликаций

$(QL, AR)[[G(V,E), Res, WE]] \Rightarrow SA,$ то есть получаемая от объекта информация позволяет выполнить определенный набор действий *SA*. Фактически это представляет собой отношения *sROd* и *sROh*. В отношении которых сделаем предположение об их эквивалентности и которые могут быть описаны импликацией:

$$(sROd \cong sROh)[[G(V,E) \to Res \to WE \to SA \to ME]] \quad (3)$$

В (3) величина *ME* представляет собой множество событий и сообщений в ИС и ее компонентах, которые сопровождают действия Нарушителя и Защитника. В свою очередь, события и сообщения оказывают решающее воздействие на выбор дальнейших действий субъекта. Можно говорить, что отношения Нарушителя и Защитника с ИС описываются через следующие импликации для соответственно:

$$hROs[[ME \to SA \to Res]] \quad (4)$$

$$dROs[[ME \to SA \to (G(V,E) \vee Res)]] \quad (5)$$

Схема, иллюстрирующая импликации (3 – 5) приведена на рисунке 2. Данные выражения можно трактовать как воздействие субъекта на объект, которое подчиняется следующему допущению:

— Нарушитель может воздействовать только на узлы ИС в части манипуляции их ресурсами;
— Защитник помимо манипуляций с ресурсами узлов может и манипулировать структурой ИС (прежде всего доступными связями узлов).

С другой стороны, сделанные предположения относительно отношений субъектов и объекта позволяют в рамках категорного подхода описать взаимодействие субъектов и объекта в виде коммутативной диаграммы, представленной на рисунке 3, где:

$Sel(SA)$ – функция выбора субъектом одного из доступных действий;

$Gen(ME)$ – функция генерации событий и сообщений в объекте;

$Ref(ME)$ – функция анализа субъектом получаемой информации.

Из диаграммы рисунке 3 и выражений (3 – 5) следует, что достижение целей Защитником и Нарушителем обусловлено их отношениями с объектом с учетом направленности этих отношений, соответственно *dROs* и *sROd* для Защитника, а также *hROs* и *sROh* для Нарушителя:

$$dROs \cup sROd = \quad (6)$$
$$= \{Ref^d(ME) \circ Gen(ME) \circ Sel^d(SA^d)\}$$

$$hROs \cup sROh = \quad (7)$$
$$= \{Ref^h(ME) \circ Gen(ME) \circ Sel^h(SA^h)\}$$

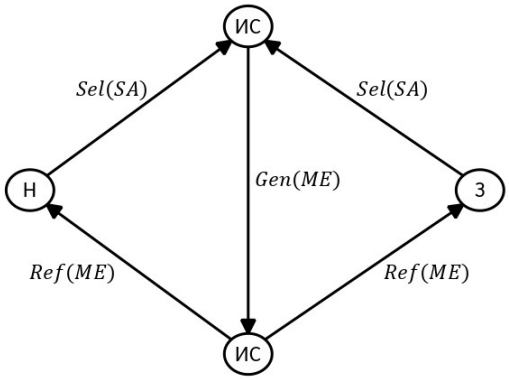

Рис. 3. Коммутативная диаграмма

Выражения (6 – 7) можно трактовать как взаимодействие субъекта с объектом, направленное на формирование требуемого с точки зрения целеполагания субъекта состояния объекта. Обозначим субъекта как $x \in AS$, тогда можно представить взаимодействие субъекта с объектом как:

$$FOS = xROs \cup sROx = \quad (8)$$
$$= Gen(ME) \to Ref(ME) \to Sel(SA)$$

На коммутативной диаграмме на рисунке 3 можно выделить два эквивалентных пути, обобщенно описывающие взаимодействие Нарушителя и Защитника: $Ref(ME) \circ Gen(ME) \circ Sel(SA)$. Относительно этих путей отметим следующее.

1. В выражении (6 – 7) множество событий и сообщений *ME* и функция их генерации в ИС $Gen(ME)$

являются общими для Защитника и Нарушителя, поскольку удаление функции $Gen(ME)$ нарушит коммутативность диаграммы (см. рисунок 3). Данное утверждение также вытекает из того факта, что генерация событий и сообщений в ИС целиком и полностью определяется характеристиками узлов ИС $VRes$.

2. Генерация и анализ событий и сообщений в ИС являются фактически единственным способом для Нарушителя или Защитника определить текущие действия оппонента и оценить результаты собственных действий. С этой точки зрения в самом общем случае каждый компонент ИС находится в совместном использовании всеми субъектами множества AS.

3. События и сообщения генерируются в каждом узле ИС единой функцией $Gen(ME)$, но собственный перечень событий и сообщений доступный для Защитника и Нарушителя может различаться. Пусть X^h – множество событий и сообщений доступных Нарушителю, а X^d – соответственно для Защитника, тогда $ME = X^h \cup X^d$, $X^h \cap X^d \neq \varnothing$, что влечет за собой $Gen(X^d) \neq Gen(X^h)$ и $Ref^d(X^d) \neq Ref^h(X^h)$.

4. Функции выбора возможных действий Защитником и Нарушителем зависят, согласно выражениям (4 – 5), от результатов функции анализа для событий и сообщений и можно утверждать $Ref^d(ME) \neq Ref^h(ME) \Rightarrow Sel^h(SA^d) \neq Sel^h(SA^h)$.

Таким образом, в качестве промежуточного итога рассмотрения процесса $OP(GS, \overline{GS}) = (dROs \cup sROd) \wedge (hROs \cup sROh)$ укажем факт асимметрии области определения образующих его отношений «субъект – объект» для Защитника и Нарушителя. При этом, как говорилось ранее и как следует из диаграммы на рисунке 3, отношения «субъект – субъект» симметричны и эквивалентны $dRSh \cong hRSd$. Положим $\widehat{AS} = \{h, d\}$, $i \in \widehat{AS}$, и $\_i = \widehat{AS} \setminus i$. В соответствии с коммутационной диаграммой эти отношения образуются функциями:

$$dRSh \cong hRSd = Sel^i(SA^i) \circ Gen(ME) \circ Ref^{-i}(ME) \quad (9)$$

Соответственно, можно определить процесс взаимодействия субъекта как

$$PIS = iRS\_i = Gen(ME) \rightarrow \rightarrow Ref^{-i}(ME) \rightarrow Sel^i(SA^i) \quad (10)$$

Здесь важно отметить следующее:

1. Защитник и Нарушитель могут иметь только определенную долю уверенности в полноте и не искаженности получаемых событий и сообщений, то есть в общем виде $P(Gen(ME))$.

2. Результаты функций $Sel(SA)$ и $Ref(ME)$ Нарушителя и Защитника могут со стороны оппонента только предполагаться с определенной долей уверенности. Кроме того, собственная реализация этих функций Защитником и Нарушителем также имеет определенную долю уверенности в силу ошибок первого и второго рода. То есть имеем в самом общем виде $P(Sel(SA))$ и $P(Ref(ME))$.

В соответствии с выражениями (6 – 10) и указанной асимметрией функций введем обозначения:

$$PR^{-i} = P^i\left[Ref^{-i}(X^{-i})\right]$$

$$PR^i = P^i\left[Ref^i(X^i)\right]$$

$$PS^{-i} = P^i\left[Sel^{-i}(SA^{-i})\right]$$

$$PS^i = P^i\left[Sel^i(SA^i)\right]$$

$$PG^i = [Gen(X^i)$$

При условии, что взаимодействие Защитника и Нарушителя в ИС осуществляется пошагово $T = \{t_1, \ldots, t_n\}$и в общем случае одновременно, процесс их взаимодействия, а значит описание процесса защиты информации в ИС (information protection process, IPP) можно формализовать как:

$$IPP = OP(GS, \overline{GS}) = \bigwedge_{i \in \widehat{AS}} \{[PG^i \rightarrow (PR^i \cup PR^{-i}) \rightarrow (PS^i \cup PS^{-i})], T\} \quad (11)$$

Заметим, что аксиоматика для операций над отношениями (например, их объединение) может быть приведена позднее, после рассмотрения функции $Gen(ME)$, что подразумевает исследование отношений между узлами ИС.

Дальнейшее рассмотрение процесса *IPP* будем проводить для каждой из функций, определяющих этот процесс в соответствии с выражениями (6 – 11).

Заключение

В рамках общей цели исследования (адаптации логико-вероятностного метода для решения задач ИБ) в статье разработаны формально-логические основы для определения возможности наличия и последующего выделения фрактальных структур, присущих ИС как сложной системе. Предложено выделить в ИС метауровень, состоящий из Защитника, Нарушителя, Пользователя (субъектов) и собственно ИС как объекта защиты. Проведен анализ отношений между субъектами

и объектом защиты с использованием аппарата математических и логических отношений. Определены типы отношений «субъект-субъект», «субъект-объект» и приведена базовая аксиоматика отношений с учетом требований по защите информации. На основе аксиоматики даны формальные логические определения основных элементов информационной безопасности: нарушитель, защитник, пользователь, внутренний нарушитель, атака, защита, противоборство. По результатам анализа отношений показано, что нарушитель и защитник используют единый источник информации для принятия решений, но при этом их деятельность по оценке ситуации и выбору действий носит асимметричный характер. Проведенный анализ отношений позволил впервые дать формальное логическое описание процессов взаимодействия субъектов между собой и с объектом защиты (6 – 11).

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. 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.
15. 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.

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

Kalashnikov A.O.[7], Bugajskij K.A.[8], Birin D.S.[9], Deryabin B.O.[10], Tsependa S.O.[11], Tabakov K.V.[12]

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: *in this article, it is proposed to consider the issues of information security based on the analysis of the relationship between the subjects and the object of protection. The types of relations "subject-subject", "subject-object" are defined and the basic axiomatics of relations is given, taking into account the requirements for information protection. Based on axiomatics, formal logical definitions of the main elements of information security are given: violator, defender, user, internal violator, attack, defense, confrontation. According to the results of the analysis of relations, it is shown that the violator and the defender use a single source of information for decision-making, but at the same time their activities in assessing the situation and choosing actions are asymmetric. The analysis of the relations made it possible to give a formal logical description of the processes of interaction of subjects with each other and with the object of protection. What is the basis for the allocation of fractal structures in the information system.*

Scientific novelty: *consideration of information security issues using the apparatus of mathematical and logical relations. Development of formal logical expressions describing the interaction of the violator and the defender with each other, as well as with the object of protection.*

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

References

1. Ryabinin, I.A. Reshenie odnoj zadachi ocenki nadezhnosti strukturno-slozhnoj sistemy raznymi logiko-veroyatnostnymi metodami / I.A. Ryabinin, A.V. Strukov // Modelirovanie i analiz bezopasnosti i riska v slozhnyh sistemah, Sankt-Peterburg, 19–21 iyunya 2019 goda. – Sankt-Peterburg: Sankt-Peterburgskij gosudarstvennyj universitet aerokosmicheskogo priborostroeniya, 2019. – pp. 159-172.
2. Demin, A.V. Glubokoe obuchenie adaptivnyh sistem upravleniya na osnove logiko-veroyatnostnogo podhoda / A.V. Demin // Izvestiya Irkutskogo gosudarstvennogo universiteta. Seriya: Matematika. – 2021. – T. 38. – pp. 65-83. – DOI 10.26516/1997-7670.2021.38.65.
3. Viktorova, V.S. Vychislenie pokazatelej nadezhnosti v nemonotonnyh logiko-veroyatnostnyh modelyah mnogourovnevyh sistem / V.S. Viktorova, A.S. Stepanyanc // Avtomatika i telemekhanika. – 2021. – № 5. – pp. 106-123. – DOI 10.31857/S000523102105007X.
4. Leont'ev, A.S. Matematicheskie modeli ocenki pokazatelej nadezhnosti dlya issledovaniya veroyatnostno-vremennyh harakteristik mnogomashinnyh kompleksov s uchetom otkazov / A.S. Leont'ev, M.S. Timoshkin // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal. – 2023. – № 1(127). – pp. 1-13. – DOI 10.23670/IRJ.2023.127.27.
5. Puchkova, F.YU. Logiko-veroyatnostnyj metod i ego prakticheskoe ispol'zovanie / F.YU. Puchkova // Informacionnye tekhnologii v processe podgotovki sovremennogo specialista: Mezhvuzovskij sbornik nauchnyh trudov / Ministerstvo prosveshcheniya Rossijskoj

7 Andrey O. 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

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

9 Denis S. Birin, junior researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: birin@phystech.edu

10 Bogdan O. Deryabin, junior researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: baga_d@mail.ru

11 Sergey O. Tsependa, junior researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: tsependе.s@gmail.com

12 Kirill V. Tabakov, junior researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: tabakov2002@mail.ru

Federacii; Federal'noe gosudarstvennoe byudzhetnoe obrazovatel'noe uchrezhdenie vysshego obrazovaniya «Lipeckij gosudarstvennyj pedagogicheskij universitet imeni P.P. SEMENOVA-TYAN-SHANSKOGO». Tom Vypusk 25. – Lipeck: Lipeckij gosudarstvennyj pedagogicheskij universitet imeni P.P. Semenova-Tyan-SHanskogo, 2021. – pp. 187-193.

6. Rossihina, L.V. O primenenii logiko-veroyatnostnogo metoda I.A. Ryabinina dlya analiza riskov informacionnoj bezopasnosti / L.V. Rossihina, O.O. Gubenko, M.A. CHernositova // Aktual'nye problemy deyatel'nosti podrazdelenij UIS: Sbornik materialov Vserossijskoj nauchno-prakticheskoj konferencii, Voronezh, 20 oktyabrya 2022 goda. – Voronezh: Izdatel'sko-poligraficheskij centr "Nauchnaya kniga", 2022. – pp. 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 Mezhdunarodnaya nauchno-tekhnicheskaya i nauchno-metodicheskaya konferenciya. Sbornik nauchnyh statej. V 4-h tomah, Sankt-Peterburg, 28 fevralya – 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. – pp. 378-382.
8. Metodika kiberneticheskoj ustojchivosti v usloviyah vozdejstviya targetirovannyh kiberneticheskih atak / D.A. Ivanov, M.A. Kocynyak, O.S. Lauta, I.R. Murtazin // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO 2018): VII Mezhdunarodnaya nauchno-tekhnicheskaya i nauchno-metodicheskaya konferenciya. Sbornik nauchnyh statej. V 4-h tomah, Sankt-Peterburg, 28 fevralya – 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. – pp. 343-346.
9. Eliseev, N.I. Ocenka urovnya zashchishchennosti avtomatizirovannyh informacionnyh sistem yuridicheski znachimogo elektronnogo dokumentooborota na osnove logiko-veroyatnostnogo metoda / N.I. Eliseev, D.I. Tali, A.A. Oblanenko // Voprosy kiberbezopasnosti. – 2019. – № 6(34). – pp. 7-16. – DOI 10.21681/2311-3456-2019-6-07-16.
10. Kocynyak, M.A. Matematicheskaya model' targetirovannoj komp'yuternoj ataki / M.A. Kocynyak, O.S. Lauta, D.A. Ivanov // Naukoemkie tekhnologii v kosmicheskih issledovaniyah Zemli. – 2019. – T. 11, № 2. – pp. 73-81. – DOI 10.24411/2409-5419-2018-10261.
11. Belyakova, T.V. Funkcional'naya model' processa vozdejstviya celevoj komp'yuternoj ataki / T.V. Belyakova, N.V. Sidorov, M.A. Gudkov // Radiolokaciya, navigaciya, svyaz': Sbornik trudov XXV Mezhdunarodnoj nauchno-tekhnicheskoj konferencii, posvyashchennoj 160-letiyu so dnya rozhdeniya A.S. Popova. V 6-ti tomah, Voronezh, 16–18 aprelya 2019 goda. Tom 2. – Voronezh: Voronezhskij gosudarstvennyj universitet, 2019. – pp. 108-111.
12. Kalashnikov, A.O. Infrastruktura kak kod: formiruetsya novaya real'nost' informacionnoj bezopasnosti / A.O. Kalashnikov, K.A. Bugajskij // Informaciya i bezopasnost'. – 2019. – T. 22, № 4. – pp. 495-506.
13. Bugajskij, K.A. Rasshirennaya model' otkrytyh sistem (CHast' 1) / K. A. Bugajskij, D. S. Birin, B. O. Deryabin, S. O. Cependa // Informaciya i bezopasnost'. – 2022. – T. 25, № 2. – pp. 169-178. – DOI 10.36622/VSTU.2022.25.2.001.
14. Bugajskij, K.A. Rasshirennaya model' otkrytyh sistem (CHast' 2) / K.A. Bugajskij, I.S. Pereskokov, A.O. Petrov, A.O. Petrov // Informaciya i bezopasnost'. – 2022. – T. 25, № 3. – pp. 321-330. – DOI 10.36622/VSTU.2022.25.3.001.
15. Bugajskij, K.A. Rasshirennaya model' otkrytyh sistem (CHast' 3) / K.A. Bugajskij, B.O. Deryabin, K.V. Tabakov, E.S. Hramchenkova, S.O. Cependa // Informaciya i bezopasnost'. – 2022. – T. 25, № 4. – pp. 501-512.