ПРИМЕНЕНИЕ ЛОГИКО-ВЕРОЯТНОСТНОГО МЕТОДА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Часть 6

Калашников А. О.[1], Аникина Е. В.[2], Бугайский К. А.[3], Молотов А. А.[4]

DOI: 10.21681/2311-3456-2025-1-96-107

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. В рамках разрабатываемой модели дано определение таких понятий как оценка опасности, поверхность атаки, а также сценария сложной системы. Показано, что данные понятия могут быть количественно определены на основе соответствующих оценок состояний отношений агентов. Показана целесообразность внедрения и место специализированных агентов, обеспечивающих управление процессами мониторинга у агентов. Предложены механизмы каскадирования, обеспечивающие единый логико-функциональный подход при определении оценок опасности. Полученные результаты обеспечивают обоснованное вычисление и использования вероятностных характеристик для последующего анализа отношений между субъектами информационной безопасности на основе применения логико-вероятностного метода при анализе указанных отношений.*

Научная новизна: *рассмотрение вопросов защиты информации с использованием аппарата математических и логических отношений. Разработаны методы количественного оценивания опасности деструктивного воздействия без привлечения информации о наличии актуальных или используемых угроз как с точки зрения программного обеспечения, так и с точки зрения логической структуры ИС. Показана эквивалентность между опасностью деструктивного воздействия и текущим состоянием отношений между агентами. Разработан метод определения устойчивости оценки опасного состояния отношений. Показано, что разработанные методы оценки опасности состояний дают возможность для исключения отдельного рассмотрения ошибок первого и второго рода при оценке реальных намерений нарушителя. Разработаны подходы, позволяющие получить интегральные оценки опасности на уровне как отдельных агентов, так и различных подсистем современных информационных систем и систем в целом за счет управления составом агрегируемых оценок состояния отношений агентов.*

Вклад авторов: *Калашников А. О. выполнил постановку задачи и общую разработку модели применения логико-вероятностного метода в информационной безопасности. Бугайский К. А. и Аникина Е. В. участвовали в подготовке всех разделов статьи. Молотов А. А. участвовал в подготовке раздела о проактивном мониторинге.*

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

Введение

Данная статья является шестой из серии публикаций, посвященных исследованию вопроса применения логико-вероятностного метода при изучении вопросов защиты информации. Метод был разработан Рябининым И. А. [1, см. ссылки на соответствующую литературу там же] и приобрел популярность при проведении исследований, в том числе, связанных с анализом и оценкой рисков сложных систем. Прежде всего для решения вопросов оценки надежности работы систем и анализа 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

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

2 Аникина Евгения Владимировна, научный сотрудник лаборатории «Безопасности сложных систем» ФГБУН Институт проблем управления им. В. А. Трапезникова РАН, г. Москва, Россия. E-mail: ajanet@ipu.ru

3 Бугайский Константин Алексеевич, младший научный сотрудник лаборатории «Безопасности сложных систем» ФГБУН Институт проблем управления им. В. А. Трапезникова РАН, г. Москва, Россия. E-mail: kabuga@ipu.ru

4 Молотов Александр Анатольевич, инженер-программист Научно-внедренческого отдела 89 ФГБУН Институт проблем управления им. В. А. Трапезникова РАН, г. Москва, Россия. E-mail: alpha.sphere@ya.ru

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 тех или иных объектов. Логико-вероятностный метод также находит свое применение и 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 различных задач в области информационной безопасности (далее – ИБ).

Постановка задачи

Логико-вероятностный метод обладает достаточно обширным набором подходов и решений по работе с логическими функциями, описывающими функционирование сложных систем, какими являются современные информационные системы (далее – ИС). Исследование применимости логико-вероятностного метода для решения задач ИБ базируется на представлении ИС в виде отношений между агентами.

В рамках достижения общей цели исследования возникает задача разработки формально-логических основ для вычисления вероятности наступления возможных деструктивных последствий, возникающих в ходе взаимодействия агентов из состава ИС. Разработка таких оценок на макроуровне – по совокупной реакции вероятностных параметров, характеризующих состояния отношений конкретного агента с другими агентами из состава ИС – выполнена в настоящей статье.

Проактивный мониторинг

В предыдущих статьях цикла [12–16] была показана возможность формирования оценок состояния отношений между агентами как результата обработки событий и сообщений, формируемых информационными ресурсами и потоками каждого агента вследствие внешних воздействий со стороны других агентов, которые определены как респонденты. Такие состояния отношений $\beta R\gamma$ агента с респондентом, определяемые каждым агентом независимо, описываются базовыми характеристиками:

- $rang$ – показатель состояния отношений $\beta R\gamma$ с конкретным респондентом, выражающийся целым числом $\eta = [1,4]$;
- $prob$ – показатель вероятности $p = [0,1]$ нахождения агента с конкретным респондентом в заданном состоянии;
- $undef$ – показатель возможности ошибки $\upsilon = [0,1]$ или «размытости» границы между доводами «за» и «против» при определении состоянии агента.

Значение величины $rang$ получается в результате комплексного оценивания состояний информационных ресурсов и потоков из состава агентов и упорядочивания множества состояний $R = \{Lr,Dr,Ir,Ur\}$ по степени снижения опасности состояния следующим образом: 4 эквивалентно Dr (Нелояльное), 3 – Ir (Неопределенное), 2 – Lr (Лояльное) и 1 – Ur (Безразличное).

В основе определения каждого из возможных состояний агента лежит оценка правдоподобия гипотезы нахождения в том или ином состоянии или уровень доверия к нахождению в определенном состоянии. Таким образом, состояние отношений агент-респондентов определяется характеристиками $prob$ и $undef$, которые в самом общем виде являются отражением неопределенности относительно реальных намерений респондента. Данную неопределенность будем рассматривать с точки зрения возможного развития дальнейших воздействий на агента в наиболее опасном для нарушения конфиденциальности, целостности и доступности направлении.

Трактовка характеристики $undef$ как показателя ошибочности определяется тем, что она зависит от суммы доказательств, снижающих уверенность в результате комплексного оценивания состояния, то есть она показывает, как часто понижалась оценка состояния при комплексном оценивании.

Отметим, что характеристика $undef$ в равной степени влияет на оценку любого состояния, что позволяет рассматривать ее в качестве ошибки как первого, так и второго типа при определении именно реальных намерений респондента.

Для снижения неопределенности в оценке реальных намерений респондента у агента есть два варианта действий:

- ожидать очередного воздействия со стороны респондента;
- получить оценку состояния отношений с данным респондентом со стороны других агентов.

Рассмотрим эти варианты снятия неопределенности с помощью базовой диаграммы, приведенной на рис. 1.

На рис. 1 узлы γ и $\beta 1$, $\beta 2$ представляют респондента и агентов соответственно. Узлы $\rho 1$ и $\rho 2$ соответствуют оценкам отношений агентов с респондентом. Морфизмы $g1$ и $g2$ представляют собой функции воздействия респондента на агентов, а морфизмы

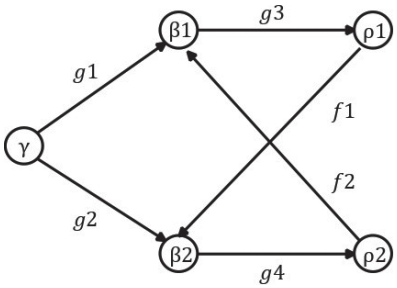

Рис. 1. Базовая диаграмма

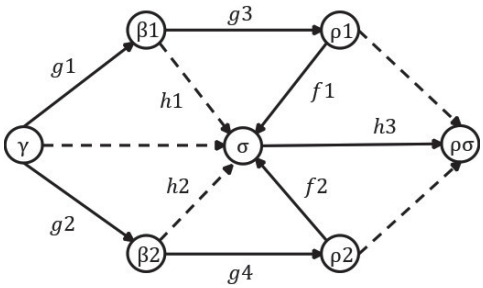

Рис. 2. Модифицированная базовая диаграмма

$g3$ и $g4$ – функции оценки состояния отношений агент – респондент.

Первый вариант фактически является реактивным и не обеспечивает своевременное реагирование на возникающие угрозы, что позволяет исключить его из дальнейшего рассмотрения.

Второй вариант включает морфизмы $f1$ и $f2$ представляющих функции обмена оценками состояния отношений агент-респондент между агентами. Существование данных морфизмов обуславливается наличием этапов разведки и внедрения, а также бокового перемещения нарушителя согласно исследовательским и аналитическим материалам, представленными организациями mitre.org и first.org.

Второй вариант, с одной стороны, обеспечивает возможности для целенаправленного сбора информации о возможных действиях нарушителя, то есть может рассматриваться как проактивный. Но, с другой стороны, необходимо отметить, что базовая диаграмма не является коммутативной в силу невозможности однозначно определить морфизмы $\beta 1 \longrightarrow \beta 2$ и $\rho 1 \longrightarrow \rho 2$.

Некоммутативность базовой диаграммы означает, прежде всего, необходимость наличия у каждого агента практически полной схемы ИС для организации обмена оценками состояний с другими агентами. Такое знание агента является для нарушителя по сути источником достаточно полной и достоверной информации о структуре ИС, что повышает успешность действий при проведении атаки. Кроме того, некоммутативность диаграммы рис. 1 резко увеличивает вычислительную нагрузку на агента, связанную с учетом оценок других агентов.

Построим на основе базовой диаграммы новую, модифицированную диаграмму, как показано на рис. 2.

Модификация базовой диаграммы заключается в ведении дополнительного узла σ и перенаправлении морфизмов f с агентов β на этот узел. На рис. 2 пунктирными линиями обозначены вспомогательные морфизмы, подтверждающие коммутативность модифицированной диаграммы.

Узел $\rho\sigma$ диаграммы может рассматриваться как оценка опасности респондента формируемой узлом σ на основании оценок $\rho 1$ и $\rho 2$, получаемых агентами в процессе их функционирования. Функция оценки опасности респондента, представленная морфизмом $h3$, будет рассмотрена далее в этой статье.

Необходимо обратить внимание на морфизмы $h1$ и $h2$, которые, с одной стороны, подтверждают коммутативность диаграммы рис. 2. Но, с другой стороны, в сочетании с морфизмами $f1$ и $f2$, по сути, не имеют на узле σ адекватной трактовки. Это дает основание продолжить модификацию базовой диаграммы. Для этого введем еще один дополнительный узел δ, на котором замкнем морфизмы $h1$ и $h2$. Это действие не нарушает коммутативности диаграммы рис. 2. Материалы, представленные организациями mitre.org и first.org, показывают, что деятельность нарушителя невозможна без использования в ИС соответствующих каналов управления захваченными агентами со стороны нарушителя. Это дает основание рассматривать морфизмы $h1$ и $h2$ как функции обнаружения таких каналов управления в исходящем трафике агентов $\beta 1$ и $\beta 2$. В итоге проведенной модификации базовой диаграммы получена коммутативная диаграмма оценки опасности респондента, представленная на рис. 3.

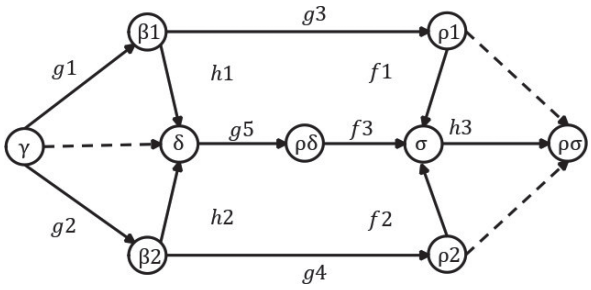

Рис. 3. Диаграмма проактивной оценки респондента

Таким образом, диаграмма на рис. 3 позволяет формировать структуру агентов, обеспечивающих проактивную оценку опасности респондента с точки зрения реальных действий нарушителя. Собственно структура агентов будет рассмотрена в этой статье ниже. На данном этапе отметим только, что для определения оценки опасности респондента должна быть

сформирована так называемая фокусная группа агентов. В состав этой группы должны входить агенты, отношения которых с респондентом базируются на физическом (наличие канала связи) и логическом (наличие протоколов обмена) уровнях. Примем, что с точки зрения состояния отношений в состав фокус-группы входят все агенты, для которых выполняется предикат $Ur = false$.

Опасность респондента

Обозначим все множество агентов из состава информационной системы как A и зафиксируем некоего агента как респондента $\gamma \in A$. Определим фокус-группу агентов для данного респондента $\gamma = const$ как Φ. Тогда условие отбора агента $\beta_i \in A$ на основании его отношения с респондентом $Q_\beta = (range,prob,undef)$ в состав фокус группы запишется как $\beta_i \in \Phi$: Q_β $(\{2,3,4\},\bullet,\bullet)$. Фокус-группа агентов по определению имеет общего респондента, который оказывает некое влияние на агентов группы. Под «опасностью респондента» будем понимать уверенность в том, что респондент может быть источником атаки. Такая уверенность, как было показано ранее, может формироваться только на основе интегральной обработки оценок состояния отношений каждого из агентов из состава группы.

В итоге имеем набор оценок как показано в табл. 1, в левой колонке которой перечислены агенты группы имеющих оценки для данного респондента.

Таблица 1.

Матрица оценок состояний отношений с респондентом

агент	*undef*	*rang*	*prob*
β_1	υ_1	η_1	p_1
β_2	υ_2	η_2	p_2
...	...	...	...
β_N	υ_N	η_N	p_N

Здесь N – число агентов в фокус-группе, $N = |\Phi|$. Каждая строка таблицы содержит величины *undef*, *rang* и *prob*, которые вычисляются каждым агентом независимо и автономно от других. То есть, в самом общем случае имеем отношения вида: $\sum_{i=1}^{N} p_i > 1$ и $\sum_{i=1}^{N} \nu_i > 1$. Отметим, что в силу особенностей процедуры комплексного оценивания мы не знаем связи между величинами rang и prob, и следует полагать, что $\forall i \in N\ p_i + \nu_i \neq 1$ для каждых отношений $\beta R \gamma$ агента с респондентом. При этом, $\forall i \in N\ 0 \leq p_i, \nu_i \leq 1$.

Для решения задачи оценки опасности респондента на ранних этапах осуществления им атаки введем функцию опасного состояния на основе параметров фокус-группы агентов:

$$Z = f(p|_\eta, \nu|_\eta) \quad (1)$$

Выражение (1) будем трактовать как определение уверенности в том, что данный набор (распределение) параметров состояний агентов может рассматриваться в качестве подтверждения опасности респондента.

Здесь необходимо сделать следующие уточнения:

1) под распределением параметров будем понимать подмножества величин *undef* и *prob*, формируемых для каждого из значений величины *rang*;
2) элементы данных множеств представляют из себя свидетельства в пользу доверия к тому или иному типу состояния респондента;
3) уверенность в опасности респондента будем определять как величину, имеющую значение при условии наличия распределения параметров.

Таким образом, с одной стороны, выражение (1) должно соответствовать условной вероятности, но, с другой стороны, приведенные выше определения для величин *rang* и *prob* не позволяют их трактовать как вероятности полной группы событий.

Вместе с тем функция опасного состояния (1) должна формировать единую шкалу оценки опасности для любых сочетаний величины *undef*, *rang* и *prob* агентов.

С учетом изложенного, используем энтропийный подход. Как известно, энтропия события X при условии наступления события Y определяется правилом Байеса:

$$H(X|Y) = H(X) - H(Y) + H(Y|X) \quad (2)$$

Дадим следующие трактовки компонентам формулы (2) применительно к поставленной задаче (1) и соответственно переопределим переменные.

$H(X|Y) \longrightarrow H(J|D)$. Представляет собой показатель наличия опасности (Jeopardy) при данном наборе (Distribution) оценок. В нашем случае это все оценки *prob* агентов, находящихся в состоянии Dr и $\overline{Lr}$. Из этих оценок посредством единой функции $g(R)$ образуем соответствующие множества оценок. Тогда функция $f(\bullet)$ от объединения этих множеств даст требуемый показатель. Отметим, что $\overline{Lr} \neq Dr$, поскольку имеет место быть отношение вида $\sum_{i=1}^{N} p_i > 1$, которые определены при описании табл. 1. В итоге можем записать

$$H(J|D) = f(g(Dr) \cup g(\overline{Lr})). \quad (3)$$

$H(Y) \longrightarrow H(D)$. По сути является показателем энтропии, то есть неопределенности источника набора оценок. В качестве источника выступает та часть агентов, которые оценивают состояние отношений с респондентом через Неопределенное состояние отношений с респондентом. То есть имеем по аналогии с (3):

$$H(D) = f(g(Ir)). \quad (4)$$

$H(Y|X) \longrightarrow H(D|J)$. Можно рассматривать как показатель достоверности появления данного набора оценок при определенной опасности или как соответствие набора оценок опасности. Отметим, что у нас нет полного описания всего множества опасностей, но поскольку величины undef и prob определены на множестве событий и сообщений агента, то мы можем говорить о полном описании множества оценок. При этом величину *undef* целесообразно рассматривать как ошибки определения состояний. Отсюда можно положить, что

$$H(D|J) = f(g(\overline{undef})). \quad (5)$$

В выражении (2) остается неопределенной переменная $H(X)$, которую можно трактовать как уверенность в том, что респондент является источником атаки. Возвращаясь к выражению (1), целесообразно говорить об оценке опасности респондента, что дает выражение

$$H(Z) = H(J|D) + H(D) - H(D|J). \quad (6)$$

Или в развернутом виде

$$H(Z) = f(g(Dr) \cup g(\overline{Lr})) + f(g(Ir)) - f(g(\overline{undef})). \quad (7)$$

Для сохранения тождественности между выражениями (6) и (7) выполним переход от вероятностных величин *undef* и *prob* к значениям энтропии. Для этого воспользуемся тем фактом, что величины в табл. 1 формируются на основе максимальных значений *prob*, а значения *undef* непосредственно связаны с ними. Следовательно, вместо этих величин будем использовать min-энтропию $H(x) = \ln(P_{max})$. С учетом особенностей логарифмической функции проведем нормировку ее переменных следующим образом: $H(x) = \ln(1 + P_{max})$.

Определим функцию $g(R)$, результатом работы которой должно быть множество оценок агентов из состава фокус-группы, находящихся в том или ином состоянии $\Phi(\cdot)$.

$$g(Dr): \forall i \in N \ln(1 + p_i) \in \Phi(Dr) \longrightarrow \eta = 4, \quad (8)$$

$$g(Ir): \forall i \in N \ln(1 + p_i) \in \Phi(Ir) \longrightarrow \eta = 3. \quad (9)$$

Далее необходимо определить аналогичные функции, содержащие логические отрицания: $g(\overline{Lr})$ и $g(\overline{undef})$. Поскольку речь идет о переходе от вероятностных величин к энтропии, воспользуемся известным выражением из теории вероятностей для чего определим единицу для выражения $p(\overline{x}) = 1 - p(x)$. Тогда, с учетом нормировки, имеем:

$$g(\overline{Lr}): \forall i \in N (2ln2 - \ln(1 + p_i) \in \Phi(Lr) \longrightarrow \eta = 2, \quad (10)$$

$$g(\overline{undef}): \forall i \in N (2ln2 - \ln(1 + v_i) \in \Phi(undef). \quad (11)$$

Поскольку каждый агент из состава фокус-группы определяет величины *undef* и *prob* автономно и независимо, то в соответствии со свойствами энтропии функция $f(\cdot)$ выражения (7) представляет собой сумму значений, получающихся в (8)–(11). Обозначим мощность множеств фокус-групп $\Phi(\cdot)$, полученных из (8)–(11) как $I(\cdot)=|\Phi(\cdot).|$. Соответственно, получаем итоговое выражение для (6):

$$H(Z) = \sum_{I(Dr)}(\ln(1 + p_i)) + \sum_{I(Lr)}(2ln2 - \ln(1 + p_i)) + \\ + \sum_{I(Ir)}(\ln(1 + p_i)) - \sum_{I(undef)}(2ln2 - \ln(1 + v_i)). \quad (12)$$

Исследуем выражение (12) для предельных случаев, когда все агенты дают единую оценку состояний отношений с респондентом.

Первый случай представляет из себя оценивание всеми агентами состояние отношения с респондентом как «Лояльно» с нулевой ошибкой, что приводит выражение (12) к виду $H(Z) = \sum_{I(Lr)}(ln2 - \ln(1 + p_i)) - \sum_{I(undef)}(2ln2 - \ln(1 + v_i))$, где $p_i = 1$, а $v_i = 0$. В результате, получаем $H(Z) = -\sum_{I(undef)}(ln2)$.

Второй случай представляет собой оценивание всеми агентами состояния отношения с респондентом как «Нелояльно» с нулевой ошибкой, что приводит выражение (12) к виду $H(Z) = \sum_{I(Dr)}(\ln(1 + p_i) - - \sum_{I(undef)}(ln2 - \ln(1 + v_i))$, где $p_i = 1$, а $v_i = 0$. В результате, при условии $I(Dr) = I(undef) = N$, получаем $H(Z) = 0$.

Кажущееся противоречие результатов в каждом из случаев обусловлено нормированием величин *undef* и *prob*. Для компенсации этого нормирования нужно ввести «нормировочную единицу» $NlnN$, что дает оценку опасного состояния на основе параметров фокус-группы агентов для выражения (1)

$$Z = NlnN - |H(Z)|, \quad (13)$$

$N = |\Phi|$ – размер фокус-группы, а величина $H(Z)$ берется по абсолютному значению для сохранения логики компенсации.

Отметим, что введение «нормировочной единицы» практически убирает зависимость оценки опасности состояния от размеров фокус-группы, что важно при практическом применении результатов оценивания в сложной системе для сравнения различных фокус-групп.

Рассмотрим предельный случай, когда размер фокус-группы равен единице. Выражение (13) в этом случае дает отрицательный результат, что противоречит общепринятому требованию о положительном значении энтропии. Следовательно, окончательный вариант вычисления опасного состояния примет вид:

$$Z = \sqrt{(NlnN - |H(Z)|)^2}. \quad (14)$$

В качестве примера фокус-группы, имеющей единичный размер, можно привести вариант использования единственного контроллера домена в ИС. Как уже отмечалось, выражение (13) для фокус-группы, состоящей из одного элемента дает отрицательный результат, показывающий невозможность проактивного мониторинга для единственного агента в ИС. Отсюда следует, что проведение проактивного мониторинга в случае единичного размера фокус-группы возможно лишь при условии введения в состав ИС дополнительных специализированных агентов, способных формировать последовательности событий эквивалентные единственному участнику фокус-группы. То есть речь идет о введении в ИС агентов-honeypot или о зеркалировании трафика на агентов с идентичными функциональными характеристиками.

В качестве промежуточного вывода укажем, что, согласно выражению (14), всегда будем иметь $Z > 0$, то есть предложенная оценка опасности соответствует реалиям ИБ, когда не существует абсолютной защиты от деструктивных воздействий.

Макроуровень

Разработанные в предыдущем разделе оценки опасности респондента позволяют перейти к рассмотрению отношений между агентами $\beta \in A$ сложной системы A на макроуровне.

В соответствии с табл. 1 примем, что множество $LC(\gamma) = \bigcup_N LC(\beta|_\gamma)$ включает в себя идентичные по характеристикам (например, одинаковый номер открытого порта) точки доступа агентов фокус-группы. На основании табл. 1 обозначим множество $Q(\gamma)$ как состоящее из векторов $[undef, rang. prob]$, получаемых каждым из агентов фокус-группы в результате оценки состояния отношений агент – респондент. Рассмотрим отношение «респондент – оценка опасности» $\gamma \longrightarrow Z$ посредством множеств с помощью диаграммы, приведенной на рис. 4.

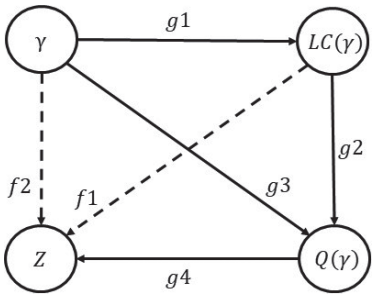

Рис. 4. Диаграмма респондент – опасность

Утверждение 1. Оценка опасности (13) является общей для данного типа точки доступа для всех агентов из состава фокус-группы.

Доказательство утверждения будем проводить на основании диаграммы респондент-опасность, приведенной на рис. 4. Морфизмы $g1$ – $g3$ соответствуют порядку формирования оценки состояния отношений агентов фокус-группы с респондентом на основе доступных респонденту точек доступа агентов. Морфизм $g4$ соответствует формированию оценки опасности респондента на базе состояний отношений агентов. Морфизмы $f1$ и $f2$ обеспечивают коммутативность диаграммы, что подтверждает утверждение. Помимо этого, выражения (1)–(13) показывают, что оценка опасности данного респондента определяется интегрально по всем оценкам состояний со стороны агентов, которые формируются на потоке событий от данных точек доступа и являются отображением возможностей нарушителя.

Отметим, что правая пара узлов диаграммы является множествами, в то время как левая пара представляется как отдельные единичные величины. Но фактически узлы левой пары также являются множествами, формирующимися во временной области:

- узел $Q(\gamma)$ на каждом из агентов может быть сформирован только на основе воздействий со стороны узла γ в течение определенного интервала времени;
- узел Z также формируется в течение заданного временного интервала.

Соответственно, узлы γ и Z диаграммы следует рассматривать как временные ряды определенной длины, что позволяет рассматривать диаграмму рис. 4 как описание пространственно-временного перехода:

- *временной ряд внешних воздействий на фокус группу агентов →;*
- *пространственная структура формирования оценок воздействий каждым из агентов →;*
- *временной ряд оценок опасности респондента.*

В дальнейших рассуждениях будем опираться на общеизвестный факт о том, что по своей сути ИС, как сложная система, естественным образом может быть представлена как мультиграф, поскольку взаимодействие агентов из ее состава основано на использовании нескольких портов и протоколов, или точек доступа, в нашем понимании, каждым из агентов.

Ранее [15-16] предлагалось отождествить респондентов с точками доступа агента. Утверждение 1 подтверждает такой подход. Сделаем следующий шаг в наших рассуждениях и обозначим:

$LC(\beta_i)$ – множество точек доступа i-го агента фокус-группы;

Φ – множество агентов фокус-группы;

$LC(\Phi)$ – множество уникальных точек доступа фокус-группы;

$LC(\beta|_\gamma)$ – множество идентичных точек доступа агентов фокус-группы.

Утверждение 2. При отображении респондента на точку доступа агента фокус-группа может быть представлена как множество уникальных точек доступа всех агентов из ее состава $LC(\Phi) = \bigcup_{i \in N} LC(\beta_i)$.

Доказательство утверждения проведем на основе диаграммы точек доступа, представленной на рис. 5.

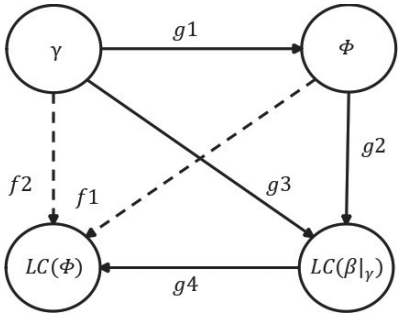

Рис. 5. Диаграмма точек доступа

Морфизмы $g1 - g3$ соответствуют пространственно-временному переходу при проведении проактивного мониторинга агентами фокус-группы. Морфизм $g4$ отображает формирование множества уникальных точек доступа группы. Морфизмы $f1$ и $f2$ обеспечивают коммутативность диаграммы, что свидетельствует в пользу истинности утверждения. В качестве дополнительного аргумента доказательства приведем следующее рассуждение. Представление фокус-группы множеством $LC(\Phi)$ полностью соответствует имеющимся моделями атак в ИБ, базирующимся на том факте, что нарушитель после установления контроля над агентом, оказывающимся в роли респондента, ограничен в своих возможностях только составом точек доступа агентов, с которыми могут быть установлены отношения и составляющих в общем случае фокус-группу.

В качестве примера рассмотрим случай, когда нарушитель-субъект находится вне пределов ИС. По результатам исследований организаций mitre.org и first.org будем полагать, что атака на ИС проводится с разных адресов. Тогда узел γ диаграммы рис. 5 представляет собой подмножество агентов, находящихся под контролем нарушителя. Что является по сути фокус-группой нарушителя, позволяющей ему оценивать свои возможности на основании реакции атакуемых агентов ИС. Соответственно, можно продолжить данное рассуждение и на случай продвижения нарушителя по структуре ИС.

Таким образом, морфизм $f2$ дает основание перейти от понятия «респондент» как атакующего агента к понятию «источник атаки», в роли которого в общем случае выступают агенты той или иной фокус-группы.

Морфизм $f1$, в свою очередь, показывает, что отдельная фокус-группа агентов может отображаться как на отдельную точку доступа, так и на несколько таких точек в случае идентичности агентов из состава группы, что позволяет определить множество точек доступа фокус-группы $LC(\Phi)$ как поверхность атаки для агентов из состава группы.

Следовательно, получаем двойственный характер фокус-группы, которая одновременно может рассматриваться как источник и как поверхность атаки. В самом общем случае это соответствует одновременной деятельности субъектов ИБ – нарушителя и защитника. В свою очередь, двойственный характер фокус-группы позволяет рассматривать выражение (14) и как оценку возможностей нарушителя, и как оценку опасности точек доступа.

Предлагаемый подход позволяет говорить о возможности декомпозиции ИС на основе фокус-групп, манипулируя которыми как источниками и поверхностью атаки, можно проводить декомпозицию до уровня отдельных агентов, выступающих в роли атакующего или защищаемого объектов.

Сделаем следующие предположения.

1. В соответствии с диаграммой проактивной оценки респондента (рис. 3) каждая фокус-группа содержит специализированные агенты, которые обозначим как:
   AL – множество агентов, обеспечивающих функции сбора и обработки событий и сообщений, что соответствует узлу δ диаграммы;
   AK – множество агентов, обеспечивающих манипулирование информационными потоками других агентов, что соответствует узлу σ диаграммы;
   AB – множество агентов, обеспечивающих функции передачи и обработки данных в ИС (то есть все узлы образующие фокус-группы), что соответствует узлу β диаграммы.
2. Каждая фокус-группа может выступать в роли источника атаки своими агентами, что согласуется с понятием сложной системы, поэтому все возможные связи между источниками и поверхностью атаки будем представлять в виде шины.

Итоговое представление ИС на макроуровне как сложной системы на основе фокус-групп приведено на рис. 6.

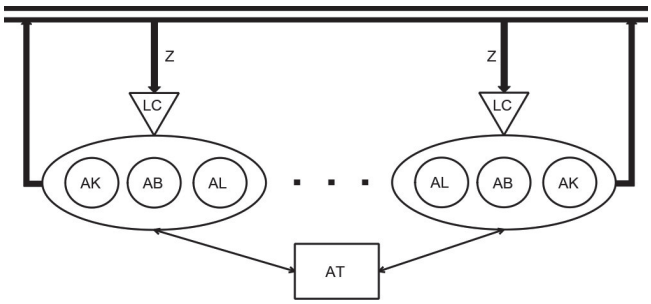

Рис. 6. Макроуровень представления ИС

Широкие стрелки на рисунке обозначают воздействие на или со стороны фокус-группы, которая представлена большим овалом. Треугольники обозначают одну или несколько точек доступа фокус-группы. Буквами Z обозначены оценки опасности точек доступа, получаемые согласно выражению (14), для каждой точки доступа каждой из фокус-групп. Кроме того, на рис. 6 показан орган управления работой фокус-групп:

AT – множество агентов, обеспечивающих функции формирования и доставки правил работы фокус-групп, прежде всего агентов типа AK и AL.

Предлагаемая концепция построения макроуровня ИС как сложной системы позволяет рассматривать ее с точки зрения распределения оценок опасности Z как по фокус-группам, так и по отдельным агентам из состава ИС.

Представляется целесообразным определить данное распределение в качестве состояния сложной системы.

Без потери общности положим, что каждая фокус-группа имеет одну точку доступа, которая испытывает внешнее воздействие со стороны одного источника. Тогда последовательность фокус-групп, представляющих ИС и испытывающих воздействия на точки доступа, может быть определена как *сценарий*. В свою очередь, сценарий может быть представлен взвешенным орграфом, как показано на рис. 7. Отметим, что связи графа сценариев определяются тем фактом, что отношения между агентами базируются на физическом (наличие канала связи и логическом (наличие протоколов обмена) уровне.

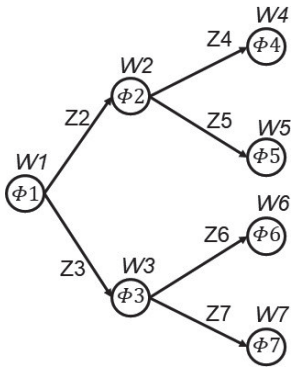

Рис. 7. Орграф сценария

На рис. 7 символом Z обозначены веса связей, определяемые выражением (14), а символом W – веса вершин графа сценария, которые определяются по аналогии с оценкой Z на основе базовых характеристик состояния отношений агентов из состава фокус-группы.

Веса вершин графа должны отражать «степень единообразия» агентов фокус-групп в формировании базовых характеристик $prob$ и $undef$. Представляется целесообразным использовать в этом качестве величину разброса величин $prob$ и $undef$ и определить вес вершины как характеристику устойчивости оценки опасности. Для этого определим два множества, объединяющих величины $prob$ – p и $undef$ – v для всех агентов из состава фокус-группы независимо от показателя состояния, то есть сформируем два различимых множества, содержащих повторяющиеся элементы. Данную операцию обозначим символом $\amalg x$. В итоге получим:

$$P = \amalg_{\beta\in\Phi} p_\beta, \quad (15)$$

$$V = \amalg_{\beta\in\Phi} v_\beta. \quad (16)$$

Величину разброса значений из множеств (15) и (16) определим как расстояние между некоей опорной точкой X и каждым из значений $p_i \in P$ и $v_i \in V$: $\mathrm{d} = (p_i \vee v_i) - X$. Отметим, что $|P| = |V| = N$ и, соответственно, $i = [1,N]$. При определении расстояния будем исходить из следующих условий:

- расстояние определяем на шкале [0,1] в соответствии с областями определения величин $prob$ и $undef$;
- одинаковые значения величин должны давать одинаковое расстояние;
- значения $prob$ должны группироваться как можно ближе к опорной точке, соответствующей «1» шкалы, что будет свидетельствовать о наибольшей согласованности наиболее вероятных оценок состояния отношений со стороны агентов из состава фокус-группы;
- значения $undef$ должны группироваться как можно ближе к опорной точке, соответствующей «0» шкалы, что также будет свидетельствовать о наименьшем числе ошибок при определении оценок состояния отношений со стороны агентов из состава фокус-группы;
- увеличение разброса значений величин $prob$ и $undef$ свидетельствует о снижении устойчивости оценок опасности фокус-группой.

Исходя из перечисленных условий определим расстояния следующим образом

$$d_p = \sum_{i=[1,N]} (p_i - 1)^2, \quad (17)$$

$$d_v = \sum_{i=[1,N]} (v_i)^2. \quad (18)$$

Выражения (17) и (18) имеют прямую аналогию с метрикой нормированного пространства, что позволяет определить «плотность» группирования (с учетом условий) как несмещенную оценку

$$\sigma_P = \sqrt{(1/\mathrm{n} - 1)d_p}, \quad (19)$$

$$\sigma_v = \sqrt{(1/\mathrm{n} - 1)d_v}. \quad (20)$$

Отметим, что одновременное увеличение результатов вычисления выражений (19) и (20) будет приводить к сокращению расстояния между распределениями, представленными множествами P и V. Определим данное расстояние как разницу интервалов

$$\mu = \frac{(p_{max} + p_{min}) - (v_{max} + v_{min})}{2}. \quad (21)$$

С учетом применяемого энтропийного подхода и особенностей логарифмической функции неопределенность устойчивости оценки опасности определится как

$$H(W) = \ln(1 + \sigma_p) + \ln(1 + \sigma_{\_v}) - ln(1 + \mu). \quad (22)$$

Максимальная неопределенность при этом будет достигаться при равномерном распределении значений *prob* и *undef* по шкале [0,1]. При максимальной концентрации величин *prob* и *undef* около границ шкалы – «1» и «0» соответственно – выражение (22) примет отрицательное значение, что обусловлено нормированием величин, получаемых из (19–23). Для компенсации этого нормирования введем «нормировочную единицу» *2ln2*, что дает следующее выражение для определения устойчивости оценки опасного состояния на основе параметров фокус-группы агентов

$$W = 2\ln 2 - |H(W)|. \quad (23)$$

В качестве промежуточного вывода укажем, что, согласно выражению (23), всегда будем иметь $W > 0$, то есть некоторую устойчивость оценки опасности, поскольку в основе расчета опасности лежат реальные события и сообщения, формируемые внешним воздействием.

Еще один вывод заключается в следующем. Поскольку веса ребер и вершин орграфа сценария, приведенного на рис. 7, изменяются во времени по мере развития атаки, то этот факт подтверждает оправданность использования принципа пространственно-временного перехода.

В качестве простейшего подхода к формированию фокус-группы приведем пример на основании таких параметров, описывающих точки доступа, как шлюз по умолчанию, номер и маска подсети агентов. В результате мы можем определить опасность именно точек доступа агентов фокус-группы по результатам внешнего воздействия, который при этом представляет собой несколько различных агентов-нарушителей, осуществляющих доступ к агентам фокус-группы через единую точку – входной шлюз. При этом все агенты группы, имеющие данный тип точки доступа, «стягиваются» в один узел трансформируемого графа ИС. То есть подмножество агентов фокус-групп ИС замещаем набором подмножеств из точек доступа, что позволяет говорить о декомпозиции сложной системы.

Еще один подход к декомпозиции заключается в выделении слоев ИС как сложной системы. Поскольку множества LC(Ф) для каждой фокус-группы, сформированной в ИС, содержат пересекающиеся (и ограниченные) наборы точек доступа, то это дает возможность для представления ИС в виде слоев, содержащих точки доступа одного типа из состава всех фокус-групп ИС. При этом представляет интерес исследование структуры слоев на предмет наличия изолированных или слабо соединенных кластеров, а также обязательных переходов нарушителя между слоями при проведении атаки.

Отметим, что использование сценариев дает возможность для моделирования действия субъекта-нарушителя, а использование слоев позволяет моделировать действия субъекта-защитника, особенно в случаях проведения атак на фиксированные точки доступа.

В любом случае декомпозиция создает условия для опережающей реакции по всем узлам ИС на используемые нарушителем порты и протоколы – точки доступа, что важно в условиях автоматизации деструктивной деятельности. Отличительной чертой предлагаемой декомпозиции является возможность применения единого функционально-логического подхода на всех уровнях – от ИС в целом до отдельных агентов только за счет манипулирования составом подмножеств точек доступа и фокус-групп.

Приведенные в статье типы агентов позволяют рассматривать ИС как систему, состоящую из фокус-групп, каждая из которых имеет в своем составе специализированных агентов, обеспечивающих управление мониторингом и потоками остальных агентов.

Заключение

В рамках общей цели исследования (адаптации логико-вероятностного метода для решения задач ИБ) в статье разработаны формально-логические основы определения количественных и качественных оценок состояний отношений функционально однородных агентов в многоагентных системах как результат агрегирования состояний отдельных агентов. Данные оценки закладывают основы для последующего применения логико-вероятностного метода при рассмотрении вопросов защиты информации в многоагентных системах. Предлагаемые механизмы количественного и качественного оценивания состояния отношений агентов позволяют проводить декомпозицию физической и логической структуры современных ИС как сложных систем. При этом, созданы условия для использования при организации ИБ подходов и методов, лежащих в основе искусственных иммунных систем.

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. Облаченко // 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. Применение логико-вероятностного метода в информационной безопасности (Часть 1) / А. О. Калашников, К. А. Бугайский, Д. С. Бирин, Б. О. Дерябин, С. О. Цепенда, К. В. Табаков // Вопросы кибербезопасности. – 2023. – № 4 (56). – С. 23–32. DOI:10.21681/2311-3456-2023-4-23-32.*
13. *Калашников А. О. Применение логико-вероятностного метода в информационной безопасности (Часть 2) / А. О. Калашников, К. А. Бугайский, Е. И. Аникина, И. С. Перескоков, Ан. О. Петров, Ал. О. Петров, Е. С. Храмченкова, А. А. Молотов // Вопросы кибербезопасности. – 2023. – № 5 (57). – С. 113–127. DOI:10.21681/2311-3456-2023-5-113-127.*
14. *Калашников А. О. Применение логико-вероятностного метода в информационной безопасности (Часть 3) / А. О. Калашников, К. А. Бугайский, Е. И. Аникина, И. С. Перескоков, Ан. О. Петров, Ал. О. Петров, Е. С. Храмченкова, А. А. Молотов // Вопросы кибербезопасности. – 2023. – № 6 (58). – С. 20–34. DOI: 10.21681/2311-3456-2023-6-20-34.*
15. *Калашников А. О. Применение логико-вероятностного метода в информационной безопасности (Часть 4) / А. О. Калашников, Е. В Аникина, К. А. Бугайский, Д. С. Бирин, Б. О. Дерябин, С. О. Цепенда, К. В. Табаков // Вопросы кибербезопасности. – 2024. – № 3 (61). – С. 23–32. DOI: 10.21681/2311-3456-2024-3-23-32.*
16. *Калашников А. О. Применение логико-вероятностного метода в информационной безопасности (Часть 5) / А. О. Калашников, Е. В Аникина, К. А. Бугайский, Д. С. Бирин, Б. О. Дерябин, С. О. Цепенда, К. В. Табаков // Вопросы кибербезопасности. – 2024. – № 4 (62). – С. 26–37. DOI: 10.21681/2311-3456-2024-4-26-37.*

APPLICATION OF THE LOGICAL-PROBABILISTIC METHOD IN INFORMATION SECURITY. Part 6

Kalashnikov A. O.[5], Anikina E. V.[6], Bugaisky K. A.[7], Molotov A. A.[8]

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

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. Within the framework of the developed model, the definition of such concepts as hazard assessment, attack surface, as well as the scenario of a complex system is given. It is shown that these concepts can be quantified on the basis of appropriate assessments of the states of agents' relationships. The expediency of the introduction and the place of specialized agents providing control of monitoring processes for agents is shown. Cascading mechanisms are proposed to provide a unified logical and functional approach to determining hazard assessments. The obtained results provide a reasonable calculation and use of probabilistic characteristics for the subsequent analysis of relations between subjects of information security based on the application of the logical-probabilistic method in the analysis of these relations.*

Scientific novelty: *consideration of information security issues using the apparatus of mathematical and logical relations. Methods have been developed for quantifying the danger of destructive impact without involving information about the presence of actual or used threats both from the point of view of software and from the point of view of the logical structure of the IP. The equivalence between the danger of destructive effects and the current state of relations between agents is shown. A method for determining the stability of the assessment of the dangerous state of relations has been developed. It is shown that the developed methods for assessing the danger of states make it possible to exclude separate consideration of errors of the first and second kind when assessing the real intentions of the violator. Approaches have been developed to obtain integrated hazard assessments at the level of both individual agents and various subsystems of modern information systems and systems as a whole by managing the composition of aggregated assessments of the state of agents' relationships.*

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 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.*

5 Andrey O. Kalashnikov, Dr. Sc. (Eng), Chief Researcher, Laboratory of Complex Systems Safety, V. A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Moscow, Russia. E-mail: aokalash@ipu.ru

6 Evgeniya V. Anikina, Researcher, Laboratory of Complex Systems Safety, V. A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Moscow, Russia. E-mail: ajanet@ipu.ru

7 Konstantin A. Bugaisky, Junior Researcher, Laboratory of Complex Systems Safety, V. A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Moscow, Russia. E-mail: kabuga@ipu.ru

8 Alexander A. Molotov, Software Engineer of the Research and Implementation Department 89 of the V. A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Moscow, Russia. E-mail: alpha.sphere@ya.ru

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. Primenenie logiko-veroiatnostnogo metoda v informatsionnoi bezopasnosti (Chast 1) / A. O. Kalashnikov, K. A. Bugaiskii, D. S. Birin, B. O. Deriabin, S. O. Tsependa, K. V. Tabakov // Voprosy kiberbezopasnosti. – 2023. – №4(56). – pp. 23–32. DOI:10.21681/2311-3456-2023-4-23-32.*
13. *Kalashnikov A. O. Primenenie logiko-veroiatnostnogo metoda v informatsionnoi bezopasnosti (Chast 2) / A. O. Kalashnikov, K. A. Bugaiskii, E. I. Anikina, I. S. Pereskokov, An. O. Petrov, Al. O. Petrov, E. S. Khramchenkova, A. A. Molotov // Voprosy kiberbezopasnosti. – 2023. – №5(57). – pp. 113–127. DOI:10.21681/2311-3456-2023-5-113-127.*
14. *Kalashnikov A. O. Primenenie logiko-veroiatnostnogo metoda v informatsionnoi bezopasnosti (Chast 3) / A. O. Kalashnikov, K. A. Bugaiskii, E. I. Anikina, I. S. Pereskokov, An. O. Petrov, Al. O. Petrov, E. S. Khramchenkova, A. A. Molotov // Voprosy kiberbezopasnosti. – 2023. – №6(58). – pp. 20–34. DOI: 10.21681/2311-3456-2023-6-20-34.*
15. *Kalashnikov A. O. Primenenie logiko-veroiatnostnogo metoda v informatsionnoi bezopasnosti (Chast 4) / A. O. Kalashnikov, K. A. Bugaiskii, E. I. Anikina, I. S. Pereskokov, An. O. Petrov, Al. O. Petrov, E. S. Khramchenkova, A. A. Molotov // Voprosy kiberbezopasnosti. – 2024. – №3 (61). – pp. 23–32. DOI: 10.21681/2311-3456-2024-3-23-32.*
16. *Kalashnikov A. O. Primenenie logiko-veroiatnostnogo metoda v informatsionnoi bezopasnosti (Chast 5) / A. O. Kalashnikov, K.A. Bugaiskii, E. I. Anikina, I. S. Pereskokov, An. O. Petrov, Al. O. Petrov, E. S. Khramchenkova, A. A. Molotov // Voprosy kiberbezopasnosti. – 2024. – №4 (62). – pp. 26–37. DOI: 10.21681/2311-3456-2024-4-26-37.*