ПРИМЕНЕНИЕ ЛОГИКО-ВЕРОЯТНОСТНОГО МЕТОДА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Часть 4

Калашников А. О.[1], Аникина Е. В.[2],Бугайский К. А.[3], Бирин Д. С.[4], Дерябин Б. О.[5], Цепенда С. О.[6], Табаков К. В.[7]

DOI: 10.21681/2311-3456-2024-3-23-32

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. Показано, что состояние отношений агента может быть получено на основе соответствующих оценок состояний на уровне информационных ресурсов и информационных потоков. Показано, что оценка состояний может быть проведена как на качественном, так и на количественном уровнях, на основе формируемых в агенте, в результате внешних воздействий, наборов событий и сообщений. Полученные результаты обеспечивают обоснованное вычисление и применение вероятностных характеристик для последующего применения логико-вероятностного метода при анализе указанных отношений.*

Научная новизна: *показана возможность определения количественных и качественных оценок состояния агента на основе формируемых в процессе функционирования событий и сообщений. Разработаны методы оценивания состояний отношений на уровне информационных ресурсов и информационных потоков через уровень доверия. Определена нижняя оценка уровня доверия к нахождению объекта в определенном состоянии. Исследованы соотношения между событиями и сообщениями из состава шаблонов состояний и текущего набора, что может быть использовано в качестве критериев при проектировании соответствующих подсистем ИС и их компонент с точки зрения информационной безопасности.*

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. Бирин Д. С. и Дерябин Б. О. участвовали в подготовке раздела о формировании меры доверия. Цепенда С.О. и Табаков К.В. участвовали в подготовке раздела о доверии к состоянию объекта.*

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

APPLICATION OF THE LOGICAL-PROBABILISTIC METHOD IN INFORMATION SECURITY. Part 4

Kalashnikov A. O.[8], Anikina E. V.[9],Bugajskij K. A.[10], Birin D. S.[11], Deryabin B. O.[12], Tsependa S. O.[13], Tabakov K. V.[14]

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 Аникина Евгения Владимировна, научный сотрудник, институт проблем управления им. В. А. Трапезникова РАН. E-mail: ajanet@ipu.ru
3 Бугайский Константин Алексеевич, младший научный сотрудник, институт проблем управления им. В. А. Трапезникова РАН. E-mail: kabuga@ipu.ru
4 Бирин Денис Сергеевич, младший научный сотрудник, институт проблем управления им. В. А. Трапезникова РАН. E-mail: birin@phystech.edu
5 Дерябин Богдан Олегович, младший научный сотрудник, институт проблем управления им. В. А. Трапезникова РАН. E-mail: baga_d@mail.ru
6 Цепенда Сергей Олегович, младший научный сотрудник, институт проблем управления им. В. А. Трапезникова РАН. E-mail: tsepende.s@gmail.com
7 Табаков Кирилл Викторович, младший научный сотрудник, институт проблем управления им. В. А. Трапезникова РАН. E-mail: tabakov2002@mail.ru

8 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
9 Eugenia V. Anikina – research fellow, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. E-mail: ajanet@ipu.ru
10 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
11 Denis S. Birin – junior researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. E-mail: birin@phystech.edu
12 Bogdan O. Deryabin – junior researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. E-mail: baga_d@mail.ru
13 Sergey O. Tsependa – junior researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. E-mail: tsepende.s@gmail.com
14 Kirill V. Tabakov 3 junior researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. E-mail: tabakov2002@mail.ru

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. It is shown that the state of the agent's relations can be obtained on the basis of appropriate assessments of states at the level of information resources and information flows. It is shown that the assessment of states can be carried out at both qualitative and quantitative levels, based on sets of events and messages formed in the agent as a result of external influences. The obtained results provide a reasonable calculation and application of probabilistic characteristics for the subsequent 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. The possibility of determining quantitative and qualitative assessments of the agent's condition based on events and messages generated in the process of functioning is shown. Methods for assessing the state of relations at the level of information resources and information flows through the level of trust have been developed. A lower estimate of the level of confidence in finding an object in a certain state has been determined. The relationships between events and messages from the state templates and the current set are investigated, which can be used as criteria in the design of the corresponding IS subsystems and their components from the point of view of information security.*

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

Введение

Данная статья является четвертой 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 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). В рамках достижения общей цели исследования (адаптации логико-вероятностного метода для решения задач ИБ) возникает задача разработки формально-логических основ для вычисления вероятностных параметров характеризующих истинность логических высказываний Разработка таких вероятностных параметров на системном уровне выполнена в настоящей статье.

Общие положения

Приведем основные положения предыдущих статей цикла [12–14], которые необходимы для решения поставленной задачи.

1. События и сообщения (далее – события) являются следствием внешнего воздействия на агента со стороны других агентов, участвующих в обмене информацией (далее – респондентов). Эти события образуют множество ME и определяют состояние отношений между агентом β и его респондентом γ. Такие состояния отношений $\beta R\gamma$ агента с респондентом (далее – состояния) было предложено представлять множеством $R = \{Lr,Dr,Ir,Ur\}$, где Lr означает Лояльное, Dr – Нелояльное, Ir – Неопределенное и Ur – Безразличное.
2. Агент представляет из себя набор информационных ресурсов (далее – ИР) и информационных потоков (далее – ИП), обеспечивающих обработку определенной категории данных в интересах субъекта, представленного аккаунтом ИС. В дальнейшем все ИП и ИР агента будем определять как объекты. Обозначим через K множество объектов в составе агента.
3. События формируются алгоритмически и независимо каждым из объектов агента. Обозначим через M_k полный набор событий, алгоритмически предопределенный на этапе разработки объекта $k \in K$. Тогда имеем: $ME = \bigcup_K M_k$.
4. События формируются разными источниками (например, один и тот же ИР может иметь более одного журнала регистрации событий), каждый из которых может иметь собственную семантику. Для единообразного описания событий было предложено все события ортогонализировать за счет введения пространства признаков с едиными шкалами параметров для каждого признака.
5. Для каждого объекта $k \in K$ и для каждого из возможных состояний агента $r \in R$ экспертным методом определяется эталонный набор событий (далее – шаблон) в виде матрицы свертки событий: V_k^r, то есть, наборы событий образуют иерархию $V_k^r \subseteq M_k^r \subseteq ME$.

Таким образом, определение состояния отношения агент-респондент $\beta R\gamma$ как реакцию агента на внешние воздействия возможно только на основе заранее заданного и фиксированного набора событий, формируемых независимо каждым из объектов.

Здесь необходимо отметить следующие особенности наборов событий объекта:

- полные наборы событий M_k формируются разработчиками на основе их понимания необходимости и достаточности именно такого набора событий для описания функционирования объекта и его состояний, что не всегда коррелируется с описанием внешнего воздействия с точки зрения ИБ;
- шаблоны V_k^r создаются экспертами исходя из их знаний и предпочтений, а также понимания особенностей функционирования данной ИС с точки зрения защиты информации;
- как показывает практика обеспечения ИБ, практически повсеместно в процессе сопоставления некоторых событий внешним воздействиям, эксперты используют такой параметр как «значимость» события для определения того или иного состояния, что неизбежно вызывает разночтения при оценке состояний.

Следовательно, можно говорить о предопределенной неполноте информации при определении состояния агента или *вероятностном характере* определения этих состояний. В связи с чем отметим следующие проблемы, связанные с понятием «вероятность» в ИБ.

Прежде всего обозначим, что общепринятый в естественно-научной среде частотный подход к определению вероятности практически не применим в ИБ, в силу того, что невозможно обеспечить повторяемость опыта (атаки) при постоянных параметрах контролируемой среды, которая является многозадачной и многопользовательской вычислительной системой [15, 16].

С одной стороны, события, как реакция на внешнее воздействие, формируются разными и независимыми источниками, а с другой стороны – для определения состояния могут быть необходимы цепочки событий, в том числе от одного источника [17, 18]. То есть, возникает проблема трактовки терминов «зависимость/независимость» и «совместность/несовместность» событий, что принципиально для определения вероятностных характеристик отношений $\beta R\gamma$.

Для уточнения постановки задачи в данной части статьи дадим следующую формулировку:

> *В условиях предопределенной неполноты исходных данных вероятность нахождения агента в том или ином состоянии отображает степень правдоподобности вычисляемого на основании зарегистрированных событий состояния отношения агента реальному внешнему воздействию со стороны респондента.*

Из сказанного выше следует, что источником неопределенности или вероятностного характера состояния агента являются независимо формируемые каждым из объектов наборы событий. При этом за счет ортогонализации событий как шаблоны, так и текущий набор, вызванный конкретным внешним воздействием, могут быть представлены матрицами свертки событий для каждого объекта. В дальнейшем, поскольку мы будем рассматривать вероятностные характеристики объекта, то индекс, указывающий на конкретный объект агента, будем опускать.

Формирование меры доверия

Экспертный метод формирования шаблонов V_i на основании предопределенного набора событий объекта можно представить следующей схемой: формирование предположений о возможных вариантах внешнего воздействия, а затем определение набора событий, которые могут возникнуть при том или ином внешнем воздействии. То есть формирование полного набора шаблонов для объекта равносильно формированию на основе экспертных заключений всех возможных гипотез $H = \{h_1,\cdots,h_n\}$ о внешнем воздействии. Это дает основание рассматривать шаблоны V_i как гипотезы: $V_i \equiv h_i$. Поскольку формирование шаблонов выполняется экспертным методом, то речь может идти о рациональной степени уверенности в истинности гипотезы на основе некоего доказательства. Положения предыдущего раздела позволяют определить в качестве такого доказательства уровень квалификации экспертов. Что, в свою очередь, говорит об эпистемологическом характере понятия «истинность гипотезы». Вопрос определения квалификации экспертов давно и активно исследуется, поэтому мы не будем его подробно рассматривать в данном исследовании.

В рамках текущего исследования под рациональной степенью уверенности в истинность гипотезы будем понимать меру доверия. В основе которой лежит тот факт, что одно или несколько событий могут одновременно входить в несколько шаблонов, описывающих различные внешние воздействия на основе имеющегося набора событий объекта: $\Sigma|V_i| > |M_r|$. То есть, шаблоны представляют собой «неопределенные» подмножества множества событий объекта. В данном случае не используется типичный для подобных ситуаций термин «нечеткое множество» поскольку факт вхождения события в то или иное подмножества должен трактоваться однозначно, но при этом подмножества не имеют четких границ, позволяющих утверждать отсутствие пересечения этих подмножеств. То есть, за счет наличия общих элементов границы между подмножествами не могут быть определены четко. Иными словами, каждая из сформированных экспертным методом гипотез о внешнем воздействии отражает внешнее воздействие с той или иной правдоподобностью или мерой доверия.

Опыт эксплуатации современных вычислительных средств показывает, что мощность множества событий объекта $|M_r|$ всегда больше числа событий используемых для определения состояний, что дает основания сразу выделить подмножество событий $\overline{M}$ не используемых для определения состояний. Тогда определим универсум событий объекта как $U = Mr \setminus \overline{M}$, или иначе, но тождественно, как $U = \bigcup_{i=[1,N]} V_i$, где N – общее число шаблонов, описывающих состояния объекта. Поскольку $V_i \equiv h_i$, то и универсум эквивалентен набору гипотез $U \equiv H$, что позволяет привести следующие рассуждения относительно шаблонов как гипотез.

С одной стороны, чем больше событий входит в шаблон или чем он *универсальнее*, тем больше шансов, что данная гипотеза будет в той или иной степени соответствовать внешнему воздействию.

С другой стороны, чем меньше общих с другими шаблонами событий входит в данный или чем он *уникальнее*, тем более достоверно данный шаблон описывает внешнее воздействие.

Дадим аналитическое определение свойств *универсальности* и *уникальности* шаблонов и гипотез.

Универсальность шаблона или гипотезы определим как их долю в универсуме:

$$A(h_i) = \frac{|V_i|}{|U|} \quad (1)$$

Уникальность шаблона определим как долю уникальных событий в его составе. Для этого определим события, общие для данного шаблона и остальных:

$$i,j = [1,N]\ \forall j \neq i\ F(h_i) = \bigcup_j (V_i \cap V_j) \quad (2)$$

С учетом (2) доля уникальных событий в шаблоне равна:

$$B(h_i) = 1 - \frac{|F(h_i)|}{|V_i|} \quad (3)$$

Поскольку гипотезы о состоянии объекта представляют собой «неопределенные» множества, то представляется возможным определить меру доверия гипотезы как долю уникальных событий каждого из шаблонов в универсуме. Выражения (1) и (3) можно рассматривать в качестве частотного представления вероятности как универсальности, так и уникальности шаблона. Ранее в этом разделе говорилось о формировании шаблонов экспертным методом, что дает основания положить следующую последовательность действий:

- сначала эксперты формируют каждый из шаблонов, что можно представить как определение вероятности события «универсальность шаблона»;
- затем вычленяют общие для этих шаблонов событий, что можно представить как определение вероятности события «уникальность шаблона».

При этом каждый из шагов данной последовательности действий выполнятся независимо и значение одной из величин $A(h_i)$ и $B(h_i)$ не дает информации о значении другой. Следовательно, выражения (1–3) позволяют определить меру доверия для гипотезы следующим образом:

$$\mu(h_i) = \frac{|V_i| - |F(h_i)|}{|U|} \quad (4)$$

Утверждение 1. Мера доверия гипотезы $\mu(h_i)$ является вероятностной характеристикой и может рассматриваться как априорная, то есть заданная на этапе разработки, вероятность описания внешнего воздействия конкретным шаблоном на базе универсума событий.

В качестве доказательства рассмотрим следующие свойства меры доверия.

При наличии единственной гипотезы о внешнем воздействии $|V_i| / |U| = 1$ и в отсутствие не уникальных событий в гипотезе $|F(h_i)| = 0$ получаем $\mu(h_i) = 1$. В случае отсутствия в шаблоне уникальных на универсуме событий $|F(h_i)| = |V_i|$ получаем $\mu(h_i) = 0$. Таким образом, доверие к описанию внешнего воздействия $\mu(h_i) \longrightarrow 1$ по мере того, как шаблон и соответствующая ему гипотеза обеспечивают повышение универсальности и уникальности при *заданном* на этапе проектирования универсуме событий.

Отметим, что все шаблоны являются подмножествами универсума: $U = \bigcup_{i=[1,N]} V_i$, мощность которого стоит в знаменателе выражения (4). В общем случае $\sum_{i=1}^{N} |V_i| > |U|$ за счет повторного вхождения отдельных событий в разные шаблоны, но числитель выражения (4), отражающий наличие общих событий в шаблонах позволяет утверждать, что $\mu(h_i) \leq 1$. Кроме того, выражение (2) позволяет рассматривать числитель выражения (4) как подмножество $V_i' = V_i \setminus F(h_i)$. Определим долю не уникальных событий для всех шаблонов на универсуме:

$$D(h_i) = \frac{|\bigcup_{i=1}^{N} F(h_i)|}{|U|} \quad (5)$$

С учетом «неопределенного» характера подмножеств, образующих шаблоны, выражение (5) по сути является мерой доверия для гипотезы, рассматривающей только общие события универсума. Подмножества V_i' и $\bigcup_{i=1}^{N} F(h_i)$ содержат уникальные события для каждого из шаблонов и общие для всех шаблонов события, соответственно, то есть не пересекаются и с точки зрения теории вероятностей образуют группу несовместных событий в универсуме:

$$\sum_{i=1}^{N} \mu(h_i) + D(h_i) = 1 \quad (6)$$

Доказательство завершено.

Выражения (1), (3) и (5) можно применять для оценки качества как наборов событий, задаваемых на этапе проектирования, так и работы экспертов по формированию гипотез о внешнем воздействии.

Шаблоны представляют собой сформированные экспертами гипотезы о вариантах внешнего воздействия. Но в процессе функционирования агента собственно внешнее воздействие со стороны респондента не известно, что дает возможность сформулировать следующие допущения.

Д1. Внешнее воздействие вызывает формирование в качестве ответа независимо в каждом из объектов некоторого набора событий C_k, который представляет собой подмножество полного набора событий M_k, заданного на этапе разработки объекта, то есть: $C_k \subseteq M_k$.

Д2. В общем случае подмножество C_k может содержать события входящие в полный набор событий M_k, но входящие в состав универсума, объединяющего только шаблоны состояний объекта $U = \bigcup_{i=[1,N]} V_i$. Это дает основание ввести величину $C = C_k \cap U$, которую определим как «текущий набор событий».

Д3. Текущий набор событий является единым для всех возможных состояний объекта и в общем виде можно сказать, что $\forall i \; C \cap V_i \neq \emptyset$.

Д4. Будем полагать, что формирование текущего набора событий C происходит в дискретные моменты времени, между которыми этот набор не изменяется.

Текущий набор событий C представляет из себя набор доказательств внешнего воздействия. При этом соотношение с универсумом фактически характеризует универсальность доказательной базы о внешнем воздействии:

$$A(c) = \frac{|C|}{|U|} \quad (7)$$

На основании выражений (4) и (5) определим подмножество общих для всех гипотез событий из текущего набора:

$$F(c) = C \cap (\bigcup_{i=[1,N]} F(h_i)) \quad (8)$$

Тогда доля уникальных событий текущего набора, предоставляющих доказательство для всех гипотез:

$$B(c) = 1 - \frac{|F(c)|}{|U|} \quad (9)$$

Меру доверия к доказательствам, представленным текущим набором событий определим по аналогии с (4):

$$\mu(c) = \frac{|C| - |F(c)|}{|U|} \quad (10)$$

Утверждение 2. Мера доверия к доказательствам текущего набора событий $\mu(c)$ является вероятностной характеристикой и может рассматриваться как априорная, то есть заданная на этапе разработки, вероятность доказательства внешнего воздействия на базе универсума событий.

Доказательство основано на допущениях Д1 – Д4 и представленных далее свойств меры доверия $\mu(c)$.

При равенстве мощностей текущего набора и универсума $|C| / |U| = 1$ и в отсутствие в текущем наборе общих для всех гипотез событий $|F(c)| = 0$ получаем $\mu(c) = 1$. В случае отсутствия в текущем

наборе уникальных на универсуме событий $|F(c)| = |C|$ получаем $\mu(c) = 0$. Таким образом, доверие к доказательствам внешнего воздействия $\mu(c) \longrightarrow 1$ по мере того, как текущий набор событий обеспечивает повышение универсальности и уникальности при *заданном* на этапе проектирования универсуме событий.

По аналогии с выражением (5) определим долю совпадающих не уникальных событий для шаблонов и текущего набора событий: в универсуме:

$$D(c) = \frac{|F(c)|}{|U|} \quad (11)$$

Величины $\mu(c)$ и $D(c)$ определяют доли совпадающих уникальных и общих событий для шаблонов и текущего набора, то есть для не пересекающихся подмножеств, которые с точки зрения теории вероятностей образуют группу несовместных событий в универсуме, что дает:

$$\mu(c) + D(c) = 1 \quad (12)$$

Доказательство завершено.

В третьей части статьи было доказано следующее утверждение (см. [14], Утверждение 1): «*Состояние объекта определяется соотнесением текущего набора событий и эталонного набора*». Как было показано в предыдущей статье цикла [14], все события текущего набора и универсума ортогонализированы, то есть приведены к единообразному с точки зрения ИБ виду и могут быт представлены в виде матриц свертки событий.

В терминологии настоящей статьи данное утверждение можно переформулировать следующим образом.

Утверждение 3. Состояние объекта определяется выполнением операций сравнения с целью подсчета числа совпадающих элементов матрицы свертки событий текущего набора C и универсума U, представленного матрицами свертки событий шаблонов V_i.

При этом относительно универсума как набора гипотез $H = \{h_1,\cdots,h_n\}$: (в силу $V_i \equiv h_i$) необходимо отметить следующее:

- данный набор гипотез отражает все возможные внешние воздействия, то есть набор является полным;
- в каждый конкретный момент времени респондент может реализовывать только одно воздействие, соответствующее одной или нескольким гипотезам, то есть гипотезы совместны.

Из допущений *Д1 – Д4* и Утверждения 3 следует, что сравнение матриц свертки можно рассматривать как ответ объекта на внешнее воздействие, который так или иначе совпадает с каждым из шаблонов. Тогда следует предположить, что наилучшим ответом g_i на внешнее воздействие будет гипотеза h_i в наибольшей степени совпадающая с текущим набором событий. Определим события, общие для текущего набора событий и гипотезы h_i:

$$F(g_i) = C \cap V_i \quad (13)$$

Определим функцию, выражающую ответ объекта как «расстояние» между гипотезой и ответом на внешнее воздействие: $\lambda : H \times G \longrightarrow E$. В дальнейшем будем обозначать ее как $\lambda(h_i,g_i)$:

$$\lambda(h_i,g_i) = \frac{|F(g_i)|}{|V_i|} \quad (14)$$

Необходимо отметить, что из выражения (13) следует, что $|F(g_i)| \le |V_i|$, то есть выражение (14) не может иметь числитель меньший нуля.

Утверждение 4. Функция расстояния $\lambda(h_i,g_i)$ является вероятностной характеристикой и может рассматриваться как мера соответствия внешнего воздействия отдельной гипотезе о таковом воздействии, представленной эквивалентным шаблоном.

В качестве доказательства рассмотрим следующие свойства функции расстояния.

При полном совпадении матриц свертки событий текущего набора и шаблона, что в общем случае при $|C| \ge |V_i|$ тождественно $F(g_i) = V_i$, функция $\lambda(h_i,g_i) = 0$. В противном случае, когда $F(g_i) \longrightarrow \varnothing$, функция $\lambda(h_i,g_i) \longrightarrow 1$, что можно трактовать как увеличение расстояния или не совпадения элементов матриц свертки событий текущего набора и шаблона. Тогда дополнение функции расстояния до единицы можно определить как правдоподобие соответствия ответа объекта внешнему воздействию, представленному той или иной гипотезой:

$$\delta(h_i,g_i) = 1 - \lambda(h_i,g_i) \quad (15)$$

Важно отметить, что $0 < \delta(h_i,g_i) \le 1$ всегда, в силу выражения (13), которое предполагает обязательное наличие событий текущего набора и шаблона в процессе функционирования объекта.

По аналогии с выражением (5) определим долю совпадающих не уникальных событий для отдельного шаблона и текущего набора событий:

$$D(g_i) = \frac{|C \cap F(g_i)|}{|V_i|} \quad (16)$$

Несложно показать, что значение $D(g_i) \le |F(g_i)|$ и если положить $1 = |V_i| / |V_i|$ в (15), то можно определить правдоподобие ответа на гипотезу следующим образом:

$$\delta(h_i,g_i) = \frac{|F(g_i)|}{|V_i|} - D(g_i) \quad (17)$$

Доверие состояния объекта

Выражение (17) подразумевает в качестве гипотезы о внешнем воздействии некоторый шаблон, а в качестве ответа на внешнее воздействие – уникальные события текущего набора.

Напомним, что в общем виде состояние отношения является решением агента о характере и степени опасности воздействия со стороны респондента в процессе обмена данными. То есть можно говорить о решении агентом когнитивной задачи по определению сходства состояния отношения с истинными действиями респондента, которое заключается в определении вероятности нахождения агента в том или ином состоянии на основании такого сходства.

При таком подходе уникальные события текущего набора должны рассматриваться в качестве доказательств в пользу той или иной гипотезы внешнего воздействия, а каждое из возможных состояний множества R – в качестве заключения о наиболее правдоподобной гипотезе внешнего воздействия при наличии известных доказательств.

Но поскольку реальное внешнее воздействие нам не известно, то это позволяет, как следует говорить[15] только об ожидаемой достоверности определения состояния $P(r,g_i)$ как ответа на внешнее воздействие на основании Утверждения 3, и оценки правдоподобия $\delta(h_i,g_i)$. Таким образом, эти величины можно рассматривать как апостериорную эпистемологическую вероятность и оценку истинности гипотезы соответственно, что дает основание сделать следующий промежуточный вывод

- в основу определения достоверности состояния может быть положена байесовская теория принятия решений, когда достоверность определения состояния пропорциональна расстоянию (14) между гипотезой и ответом на внешнее воздействие;
- для каждого внешнего воздействия, представленного текущим набором событий C необходимо определять возможный ответ g для всех гипотез h_i в виде шаблонов V_i.

Величина $P(r,g_i)$, определяемая для каждого состояния по максимально возможному числу доказательств, может рассматриваться как потенциально наиболее правильный ответ на гипотезу о возможном реальном внешнем воздействии на объект. При условии, что данное доказательство представляется наиболее верным для данной гипотезы (Gabbay Dov M., Hartmann S., Wood J. The Development of the Hintikka Program // Handbook of the History of Logic. – 2011. – Vol. 10. – P. 311–356.). Термин «наиболее верным» на основании Утверждений 1, 2 и 4 будем определять как использование в качестве доказательств уникальных событий из состава текущего набора и шаблонов.

Как следует из выражений (6), (12) и (17), для определения величины $P(r,g_i)$ на основе байесовской теории принятия решений целесообразно дать следующие трактовки определенных ранее величин доверия и правдоподобия:

- мера доверия гипотезы $\mu(h_i)$ в качестве априорной вероятности принадлежности заданных на этапе разработки событий к определенной гипотезе о внешнем воздействии;
- мера доверия к текущему набору событий $\mu(c)$ в качестве априорной вероятности принадлежности текущего набора событий к определенному ответу на внешнее воздействие;
- истинное правдоподобие $\delta(h_i,g_i)$, как вероятность принадлежности событий текущего набора к одной из гипотез.

В итоге получаем следующее определение апостериорной вероятности правдоподобности гипотезы при наличии данных доказательств:

$$P(r,g_i) = \frac{\mu(c)\delta(h_i,g_i)}{\mu(h_i)} \qquad (18)$$

Утверждение 5. Апостериорная вероятность $P(r,g_i)$ дает оценку правдоподобия нахождения объекта в том или ином состоянии или уровень доверия к нахождению объекта в определенном состоянии.

Доказательство утверждения основано на Утверждениях 1–4, обеспечивающих вычисление степени правдоподобия ответа g объекта, представленного текущим набором событий C, гипотезам о внешнем воздействии h_i, представленными в виде шаблонов V_i, которые в свою очередь эквивалентны состояниям объекта. При этом, согласно Gabbay Dov M., Hartmann S., Wood J., апостериорная вероятность, определяемая по максимально возможному числу доказательств, может рассматриваться как потенциально наиболее правильный ответ на гипотезу о реальном внешнем воздействии на объект, если данные доказательства представляются наиболее правдоподобными для данной гипотезы.

Утверждение 6. Величина $P(r,g_i)$ является нижней оценкой уровня доверия к нахождению объекта в определенном состоянии.

Доказательство основано на том факте, что для расчета уровня доверия используются уникальные события из состава текущего набора и шаблонов, которые согласно (2–16) заведомо меньше полных составов как текущего набора событий, так и шаблонов. А поскольку формирование шаблонов, отображающих те или иные гипотезы о внешнем воздействии выполняются экспертным методом,

15 Gabbay Dov M., Hartmann S., Wood J. The Development of the Hintikka Program // Handbook of the History of Logic. – 2011. – Vol. 10. – P. 311–356.

то уникальные события образуют фиксированные на этапе разработки подмножества универсума.

В самом общем случае можно полагать, что каждый шаблон соответствует одному из состояний объекта, то есть $V_i \equiv h_i \equiv r$. Это дает возможность рассматривать величину $P(r,g_i)$ как уровень доверия для отдельных состояний $r \in R$, $R = \{Lr,Dr,Ir,Ur\}$.

Однако, внешнее воздействие в соответствии с базами данных mitre.org может относиться к разным классам по механизмам или доменам атак (CAPEC) с использованием различных типов слабых мест программного и аппаратного обеспечения (CWE) объектов из состава агента. Что дает основание представлять внешнее воздействие несколькими различными с этой точки зрения наборами шаблонов $X_i^r \subseteq M_k \subseteq ME$, $X_i = \{V_1,\cdots,V_L\}$ $i = [1,L]$ и L – число шаблонов, описывающих конкретное состояния для отдельного объекта. Несложно показать, что в рамках логико-вероятностного метода следует сделать следующее допущение.

Д5. Все шаблоны из набора, описывающего состояние объекта, образуют полную группу событий.

Тогда наборы шаблонов X^r могут рассматриваться как предикаты z_i, $i \in L$. То есть, состояние может быть представлено в виде логической формулы $r = \vee(i \in N)z_i$, что дает следующий полином $p^*(X^r) = p_1 + p_2(1 - p_1) + p_3(1 - p_2)(1 - p_1) + \cdots$, где p_i определяется согласно (18) для каждого шаблона.

Рассмотрим выражение (18), где представляет интерес отношение априорных вероятностей. С учетом выражений (4) и (10) можем записать следующее уравнение как условие получения наибольшего значения величины $P(r,g_i)$:

$$\frac{|C| - |F(c)|}{|V_i| - |F(h_i)|} = 1 \qquad (19)$$

С учетом выражений (2) и (8) на основании выражения (19) можно сделать следующие выводы:

W1. Мощность универсума не имеет принципиального значения для определения доверия к состоянию объекта.

W2. Ситуации, когда шаблон или текущий набор событий полностью состоят из общих с другими шаблонами событий, не имеют смысла при определении состояния объекта, то есть с точки зрения ИБ.

W3. Как уже отмечалось выше, $0 < \delta(g_i,h_i) \le 1$, а значит и $P(g,h) > 0$ всегда в силу (см. (13)) обязательного наличия событий текущего набора и шаблона в процессе функционирования объекта, то есть $P(r,g_i) > 0$ при $C > \Sigma_{i=1}^N F(h_i)$.

Неопределенность состояния

Как было показано в предыдущих разделах настоящей статьи, определение доверия к состоянию объекта базируется на шаблонах, представляющих ту или иную гипотезу о внешнем воздействии. Предварительно сделаем следующее допущение.

Д6. Без потери общности будем полагать, что каждое состояние объекта описывается одной гипотезой, которой соответствует один шаблон.

Все шаблоны представляют собой «неопределенные» множества, поэтому выражения (6), (12), (17) содержат величины $D(*)$, характеризующие долю не уникальных событий в шаблонах и их пересечении с событиями текущего набора. Эти общие события (2), которые не могут быть однозначно отнесены к тому или иному шаблону, создают неопределенность конкретного состояния объекта. Для определения этой неопределенности воспользуемся энтропийным подходом по аналогии с [19].

Рассмотрим условия получения предельных значений неопределенности состояния объекта на основании выражений (2), (5), (11) и (16).

Максимальная неопределенность состояния объекта $D(*) = 1$ возникает при следующих условиях:

$$\cup_{i=1}^N F(h_i) = U;$$
$$F(h) = U;$$
$$C \cap F(h_i) = V_i;$$
если $D(c) = 1$, то и $D(h_i) = 1$.

Минимальная неопределенность состояния объекта $D(*) = 0$ возникает при следующих условиях:

$$\cup_{i=1}^N F(h_i) = \varnothing;$$
$$C \cap (\cup_{i=1}^N F(h_i)) = \varnothing;$$
$$C \cap F(h_i) = \varnothing.$$

Обобщая перечисленные условия, можно вывести следующие свойства неопределенности для отдельного состояния $D(r)$.

$$D(r) = 0 : (V_i = U) \vee (F(h_i) = \varnothing \wedge (V_i \subset U)) \qquad (20)$$

$$D(r) = 1 : (F(h_i) \cap V_i = V_i) \wedge (V_i \subset U)) \qquad (21)$$

Выражение (20) означает, что минимум неопределенности состояния достигается, когда все события универсума принадлежат единственному шаблону или, когда шаблон не содержит общих со всеми другими шаблонами событий из состава универсума.

Соответственно, выражение (21) показывает, что максимум неопределенности состояния достигается, когда шаблон состоит только из общих с другими шаблонами событий.

Напомним, что $D(h_i)$ представляет собой долю общих событий для всех состояний объекта или значение общей неопределенности всех состояний, а $D(c)$ – это значение общей неопределенности для всех состояний в ответе объекта на внешнее воздействие. Соответственно, эти значения можно рассматривать как априорные и апостериорные величины. При таком подходе представляет интерес случай, когда $D(c) = D(h_i)$. На основании выражений (5) и (11) можно вывести, что $F(c) = \cup_{i=1}^N F(h_i)$

и с учетом (8) получаем $C \cap (\cup_{i=1}^{N} F(h_i) = \cup_{i=1}^{N} F(h_i)$. Из чего следует, что $C = (\cup_{i=1}^{N} F(h_i)$. На основании чего с учетом (2) и (19) можно сделать следующий вывод:

W4. Для определения состояния объекта между текущим набором событий и общими событиями отдельного шаблона V_i, описывающих гипотезы о внешнем воздействии необходимо выполнение условия:

$$\min|C| = \Sigma_{i=1}^{N} |F(h_i)| \quad (22)$$

Выражение (22) также, как и выражения (1), (3) и (5), можно применять для оценки качества как наборов событий, задаваемых на этапе проектирования, так и работы экспертов по формированию гипотез о внешнем воздействии. Соответственно, представляет интерес дальнейшее исследование соотношения шаблонов и текущего набора на основе данных выражений как риск-ориентированного критерия в ИБ.

Согласно (13) по результатам внешнего воздействия мы имеем $F(g_i) = C \cap V_i$ и соответственно, $F(g_i) \subseteq V_i$ Следовательно, целесообразно положить, что уменьшение доли событий шаблона, совпадающих с ответом объекта на внешнее воздействие, повышает неопределенность состояния. Из чего следует, что с учетом выражений (4) и (10) получаем величину, которая показывает долю неиспользованных событий из шаблона:

$$D(c,v_i) = \frac{|V_i| - |F(g_i)|}{V_i} \; (|V_i| - |F(g_i)|)/|\text{V\_i}| \quad (23)$$

На основании выражения (16) несложно показать, что по результатам внешнего воздействия $C \cap F(h_i) \subseteq F(h_i)$. Следовательно, целесообразно положить, что увеличение доли общих событий, совпадающих с ответом объекта на внешнее воздействие, повышает неопределенность состояния. Откуда по аналогии с (23) можем получить долю неиспользованных общих событий:

$$D(c,h_i) = \frac{|F(h_i)| - |C \cap F(h_i)|}{V_i} \quad (24)$$

Из (3) можем определить априори заданную на этапе разработки собственную неопределенность шаблона, которая соответствует свойству (21):

$$D(v_i) = \frac{|F(h_i)|}{V_i} \quad (25)$$

В [19] была показана возможность применения энтропийного подхода для учета неполноты информации, описывающей как гипотезы о внешнем воздействии, так и ответов на него при определении состояния объекта. Тогда выражения (23)–(25) дают основание привести следующее выражение для неопределенности состояния объекта:

$$D_r = \ln(1 + D(v_i)) - \ln(1 + D(c,h_i)) + \ln(1 + D(c,v_i)) \quad (26)$$

Рассмотрим предельные случаи, определяемые (20) и (21), для выражения (26).

Пусть $D(c,h_i) = 0$, то есть текущий набор событий включает все общие события шаблона $F(h_i) = C \cap F(h_i)$, что дает $F(h_i) \geq C \cap F(h_i)$. Для случая равенства $F(g_i) = F(h_i)$ выражение (26) может быть представлено как $[(F(h_i) + (V_i - F(h_i))] \; / \; V_i$, что дает $D_r = 1$. В случае $F(g_i) > F(h_i)$ получаем:

$$D_r = D(v_i) + D(c,v_i) \quad (27)$$

Пусть $D(c,h_i) = 1$, то есть текущий набор событий исключает все общие события шаблона $C \cap F(h_i) = \emptyset$, что дает $F(h_i) = V_i$, тогда получаем:

$$D_r = D(c,v_i).$$

Пусть $D(c,v_i) = 1$, то есть $F(g_i) = \emptyset$, что влечет $C \cap F(h_i) = \emptyset$ и $D(c,v_i) = D(v_i)$, тогда получаем:

$$D_r = 1.$$

Пусть $D(c,v_i) = 0$, то есть $F(g_i) = V_i$ и получаем, что $D(c,v_i) = 0$. Из чего следует, что для случая $F(h_i) = V_i$ имеем $D_r = 1$, а в остальных случаях $D_r = D(v_i)$.

Отметим еще раз, что $D_r = 0$ только при условии $F(h_i) = \emptyset$ и $V_i = C \cap V_i$.

Ранее отмечалось, что величину $D(v_i)$ следует рассматривать как априорно заданную на этапе разработки неопределенность состояния объекта. Если трактовать долю уникальных событий $V_i^1 = V_i \setminus F(h_i)$ как уровень подтверждения гипотезы с вероятностью равной 1, то наличие общих сообщений в шаблонах можно рассматривать как резерв, позволяющий повысить значение $P(r,g_i)$ за счет отнесения общих событий к конкретному шаблону, соответствующему конкретной гипотезе о внешнем воздействии. Подмножества V_i' и $\cup_{i=1}^{N} F(h_i)$ содержат уникальные события для каждого из шаблонов и общие для всех шаблонов события, соответственно, то есть не пересекаются и с точки зрения теории вероятностей образуют группу несовместных событий в универсуме. Тогда выражение (27) совместно с Утверждением 6 позволяет сделать следующий вывод:

W5. Уровень доверия к нахождению объекта в определенном состоянии фактически может быть определен только на интервале значений от $P(r,g_i)$ до $P(r,g_i) + P(D_r)$, где $P(D_r)$ можно рассматривать как функцию разрешения неопределенности.

Заключение

В рамках заявленной цели настоящего исследования (адаптации логико-вероятностного метода для решения задач ИБ) в статье разработаны формально-логические основы получения вероятностных оценок как результата обработки событий и сообщений, формируемых в процессе функционирования агента. Данные вероятностные оценки необходимы

для последующего определения состояний отношений агентов на основе логико-вероятностного метода при рассмотрении вопросов защиты информации в многоагентных системах. Полученные результаты показывают недостаточность собственных возможностей агента по определению состояния отношений с респондентами. Предлагаемые механизмы количественного и качественного оценивания результатов обработки событий и сообщений могут быть использованы при проектировании соответствующих подсистем современных ИС и их отдельных компонентов.

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.*
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.*
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.*
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.*
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.*
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 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. С. 23–32. 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. С. 23–32. DOI: 10.21681/2311-3456-2023-6-20-34*
15. *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.*
16. *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.*
17. *Котенко И. В. Технологии больших данных для корреляции событий безопасности на основе учета типов связей / И. В. Котенко, А. В. Федорченко, И. Б. Саенко, А. Г. Кушнеревич // Вопросы кибербезопасности. – 2017. – № 5 (24). – С. 2–16. С. 23–32. DOI: 10.21681/2311-3456-2017-5-2-16*
18. *Дойникова Е. В. Совершенствование графов атак для мониторинга кибербезопасности: оперирование неточностями, обработка циклов, отображение инцидентов и автоматический выбор защитных мер / Е. В. Дойникова, И. В. Котенко // Труды СПИИРАН. – 2018. – № 2 (57). – С. 211–240.*
19. *Калашников, А. О. Модель оценки безопасности сложной сети. (часть 1) / А. О. Калашников, К. А. Бугайский // Вопросы кибербезопасности. – 2022. – № 4 (50). – С. 26–38. DOI:10.21681/2311-3456-2022-4-26-38*