ПРИМЕНЕНИЕ ЛОГИКО-ВЕРОЯТНОСТНОГО МЕТОДА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ЧАСТЬ 3)

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

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

Метод исследования: *при проведении исследования использовались основные положения методологии структурного анализа, системного анализа, теории принятия решений, теории категорий, 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 из состава агента. Разработана схема признаков для представления событий с точки зрения информационной безопасности и предложен способ единообразного представления событий и сообщений поступающих из разных источников . Доказано, что состояние отношения на уровне информационного ресурса или информационного потока определяется как результат соотнесения текущего и эталонного наборов событий. Доказано, что события и их наборы могут быть представлены как многоместные отношения признаков. Доказано, что каждое отношение признаков для события может быть поименовано первым элементом схемы признаков. Разработана матрица свертки признаков, содержащая только разрешенные сочетания параметров признаков для наборов событий, описывающих состояние отношений. Доказано, что применение матрицы свертки дает линейную зависимость от размерности наборов событий. Даны формальные определения базовых действий Защитника и Нарушителя на агенте. Обоснована необходимость внесения изменений в состав и способы регистрации событий информационной безопасности информационных ресурсов и информационных потоков.*

Научная новизна: *рассмотрение вопросов защиты информации с использованием аппарата математических и логических отношений, а также теории категорий. Разработка матрицы свертки событий на основе категорного подхода для определения состояния отношений агента. Доказательство линейной зависимости операций сравнения текущего и эталонного наборов событий при использовании матрицы свертки событий. Разработка формальных определений базовых операций агента для Защитника и Нарушителя. Сформулированы две гипотезы, описывающие возможности агента в области защиты информации.*

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. разработали модель многоместных отношений при описании наборов событий, разработали доказательство утверждения 4, а также сформулировали гипотезы и определения базовых операций агентов. Перескоков И.С и Петров Андрей О. разработали доказательство утверждения 1. Петров Александр О. и Храмченкова Е.С. разработали доказательство утверждения 3, Молотов А.А. разработал доказательство утверждения 2.*

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

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

3 Аникина Евгения Владимировна, научный сотрудник, Институт проблем управления им. В.А. Трапезникова РАН. e-mail: ajanet@ipu.ru

4 Перескоков Илья Сергеевич, младший научный сотрудник, Институт проблем управления им. В.А. Трапезникова РАН. E-mail: pereskokov@phystech.edu

5 Петров Андрей Олегович, младший научный сотрудник, Институт проблем управления им. В.А. Трапезникова РАН. E-mail: petrovaojob@gmail.com

6 Петров Александр Олегович, младший научный сотрудник, Институт проблем управления им. В.А. Трапезникова РАН, E-mail: petrovalexandr@ipu.ru

7 Храмченкова Екатерина Сергеевна, младший научный сотрудник, Институт проблем управления им. В.А. Трапезникова РАН. E-mail: hramchenkovaes@yandex.ru

8 Молотов Александр Анатольевич, инженер-программист, Институт проблем управления им. В.А. Трапезникова РАН. E-mail: alpha.sphere@ya.ru

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

DOI: 10.21681/2311-3456-2023-6-20-34

Введение

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

1. Построение структурно-логической модели системы за счет выделения и использования событий с несовместными исходами.
2. Проведение преобразований полученных логических уравнений на основе функций булевой алгебры с целью получения системы уравнений с конечным числом переменных.
3. Теоретически обоснованный переход от уравнений булевой алгебры к уравнениям с вероятностными переменными.

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

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

Постановка задачи

Современные информационные системы (далее – ИС) [12, 13] отличаются большим разнообразием обрабатываемой информации, сложными типами связей между аппаратными и программными компонентами, распределенным характером обработки и управления информацией и компонентами ИС. Что с большой вероятностью влечет за собой проблему экспоненциального взрыва при непосредственном использования для описания структурно-логических схем ИС функций алгебры логики в рамках логико-вероятностного метода.

Для обеспечения достижения общей цели исследования (адаптации логико-вероятностного метода для решения задач ИБ) в настоящей статье разработаны формально-логические основы для предотвращения экспоненциального взрыва. Для решения этой задачи выделяется системный уровень ИС, состоящий из функций расчета состояния отношений агентов информационной безопасности.

Формализация исходных данных

Обозначим множество агентов в составе ИС как *AG*, отдельного агента как $\beta \in AG$, а множество агентов, взаимодействующих с данным и обозначаемых далее как респондентов – как *AV*, то есть имеем $AV \subset AG, \gamma \in AV, \beta \in AG, \beta \neq \gamma$.

Положения и выводы изложенные в [14, 15] показывают, что выбор тех или иных действий по защите информации для конкретного агента зависит от определения намерений каждого из респондентов, которые предложено оценивать как состояние отношения $\beta[R]_i, i = \{1, \dots, n\}, n = |AV|$ между агентом β и респондентом γ. Состояния отношений определены как $R = \{Lr, Dr, Ir, Ur\}$ или *R*={*Лояльное, Нелояльное, Неопределенное и Безразличное*} соответственно. Таким образом, интегральное состояние агента представляет собой вектор состояний отношений данного агента со всеми его респондентами

$$Q_\beta = [\beta[R]_1, \dots, \beta[R]_n], n = |AV| \quad (1)$$

При этом определение состояния отношений агент может выполнить только на основании сбора и анализа событий и сообщений, формируемых информационными потоками (далее – ИП) и информационными ресурсами (далее – ИР) из состава данного агента.

На основании [13, 16, 17, 18] можно полагать, что данные события и сообщения генерируются программным путем (автоматически) и независимо каждым ИП и ИР как результат внешних воздействий или взаимодействия собственных ИП и ИР, но опять же вызванных внешними воздействиям. Обозначим множество ИП в составе агента как *QS*, а множество ИР – как *QR*. Для реализации выражения (1) необходимо обеспечить разделение событий и сообщений, как по функциональному признаку, так и по респондентам. Поскольку взаимодействие агентов основано на обмене сообщениями, то обозначим MS^{β} как исходящие сообщения агента, MS^{γ} – как входящие сообщения агента. Работу агента можно представить в виде схемы $MS^{\gamma} \to (QS, QR) \to MS^{\beta}$. Соответственно, формируемые в процессе работы агента события и сообщения можно разделить по типам:

— внешние воздействия (*in*), позволяющие идентифицировать респондента и его воздействие;
— события и сообщения (*out*) от ИП и ИР, являющиеся откликом агента на внешние воздействия.

Совокупность этих типов событий и сообщений, автоматически формируемых агентом в процессе его функционирования, обозначим как $ME = \{ME^{in}, ME^{out}\}$.

Сделаем следующие допущения.

D1. В каждый конкретный момент времени формирование *ME* агента вызывает один респондент.

D2. Один и тот же респондент может воздействовать на агента разными способами, то есть оказывать воздействие на различные ИП и ИР агента.

D3. Отдельное воздействие респондента вызывает формирование событий и сообщений только частью ИП и ИР агента.

D4. Отдельное воздействие респондента вызывает формирование алгоритмически обусловленного набора событий и сообщений со стороны каждого из участвующих ИП и ИР агента.

Эти допущения дают возможность установить отображение $ME^{in} \to ME^{out}$ в виде функций воздействия $\delta: MS^{\gamma} \to ME^{in}$ и отклика $\varepsilon: ME^{out} \to MS^{\beta}$.

Таким образом, общем виде агент может быть представлен как автомат

$$\beta = \langle ME, QS, QR, \delta, \varepsilon, Q_{\beta} \rangle \qquad (2)$$

Множество *ME*, а также функции δ, ε для любых *QS* или *QR* агента входящие в выражение (2) алгоритмически предопределены на этапе разработки соответствующих ИП и ИР, а также агента в целом. Отсюда следует вывод, что реакция агента на любое внешнее воздействие со стороны респондента γ представляет собой фиксированный по составу и содержанию конечный набор событий и сообщений QM_{γ}. При этом, одни и те же комбинации событий (или отдельное событие) могут входить в подмножества *QM* описывающих разных респондентов.

$$QM_{\gamma} = ME_{\gamma}^{in} \cup ME_{\gamma}^{out},\ QM_i \cap QM_j \neq \emptyset, \qquad (3)$$

$$QM_i, QM_j \in ME,\ i, j \in AV$$

Таким образом, функционирование агента с точки зрения информационной безопасности (далее – ИБ) может быть представлена целевой функцией

$$FT: \bigcup_{\gamma \in AV} QM_{\gamma} \to Q_{\beta} \qquad (4)$$

Исходя из алгоритмической предопределенности множества *ME* любое его подмножество *QM* может быть разделено на следующие функциональные подмножества:

M^{α} – события и сообщения, позволяющие идентифицировать респондента, то есть отвечающие на вопросы «кто, где, когда»;

M^{Q} – события и сообщения, позволяющие идентифицировать состояние отношения агент-респондент, то есть отвечающие на вопрос «что делает».

В итоге имеем $QM = \{M^{\alpha}, M^{Q}\}$. При этом согласно (3) действуют следующие ограничения $\sum_{\gamma \in AV} |QM_{\gamma}| > |ME|$ и $|M_i^{\alpha}| + |M_i^{Q}| > QM_i$, $i \in AV$, которые говорят о том, что все подмножества формируемые из общего множества *ME* агента являются «неопределенными». В данном случае не используется типичный для подобных ситуаций термин «нечеткое множество» поскольку для реализации (3) и (4) факт вхождения события или сообщения в то или иное подмножества должен трактоваться однозначно, но при этом подмножества не имеют четких границ, позволяющих утверждать отсутствие пересечения этих подмножеств. Соответственно, агент должен на алгоритмическом уровне реализовывать соответствующие функции отнесения отдельных событий и сообщений к тому или иному целевому подмножеству.

Функцию выделения событий и сообщений, обеспечивающих идентификацию респондента представим в виде

$$F^{\alpha}(m): \delta(MS^{\gamma}) \to (m \in M_{\gamma}^{\alpha}) \qquad (5)$$

Результатом работы функции является набор правил $BA = \{b_i, \dots, b_n\}$, $b_i = \{0,1\}$. Значение «1» для элемента будет означать отнесение отдельного события или сообщения *m* из множества MS^{γ} к набору событий и сообщений, позволяющие идентифицировать конкретного респондента.

Это дает функцию распределения событий и сообщений – откликов агента на внешние воздействия – по взаимодействующим респондентам

$$FA(m): (ME \wedge BA) \rightarrow (m \in QM_{\gamma}) \quad (6)$$

Возникающая рекурсия между выражениями (5) и (6) заслуживает отдельного исследования.

Здесь необходимо обратить внимание на следующие условия.

Y1. Принципы построения современных вычислительных средств позволяют представить каждый из ИП и ИР агента как единый набор API и алгоритмов для всех взаимодействующих респондентов.

Y2. Регистрация событий и сообщений в процессе функционирования ИП и ИР агента реализуется разработчиком, что означает уникальность допустимых наборов событий и сообщений *M* для каждого ИП и ИР, то есть $ME = \bigcup_{i \in N} M_i$, $M_i \cap M_j = \emptyset$, $i, j \in N$,

$$M = \{M^{in}, M^{out}\}, \quad M_i^{in} \in ME^{in}, \quad M_i^{out} \in ME^{out},$$

где $N = |QS| + |QR|$ – общее число ИП и ИР в составе агента.

Y3. Не все ИП и ИР агента могут принимать участие в определении состояния отношения с конкретным респондентом.

На основании условий *Y1-Y3* можно определить функцию отнесения сообщений из множества QM_{γ} к множеству QP_i, $i \in N$

$$FM(m): (QM_{\gamma} \wedge BM) \rightarrow (m \in QP_i) \quad (7),$$

где *BM* – набор правил $BM = \{b_i, \dots, b_n\}, b_i = \{0,1\}$. Значение «1» для элемента будет означать отнесение отдельного события или сообщения *m* из множества QM_{γ} к набору событий и сообщений, описывающих реакцию агента на воздействия конкретного респондента.

Выражение (7) определяет, что множество QP содержит все события и сообщения из *QM* для отдельного ИП или ИР агента, относящиеся к определенному респонденту $QP = \{M^{\alpha}, M^{Q}\}$. При этом наличие в *QP* подмножества M^{α} обеспечивает сквозную идентификацию респондента в данном отношении для всех ИП и ИР агента. Это позволяет рассматривать *QP* как паттерн (схему) описывающую реакцию агента на внешнее воздействие посредством фиксированных наборов событий и сообщений для отдельных ИП и ИР.

Выражения (4) – (7) позволяют представить отношение агент-респондент в виде декартового произведения множеств

$$\beta[R]^{*} = QP_1 \times \cdots \times QP_i \times \cdots \times QP_N \quad (8)$$

Символ * в выражении (8) означает необходимость выбора конкретного состояния отношений. То есть, каждому состоянию отношений агента $R = \{Lr, Dr, Ir, Ur\}$ должен соответствовать определенный набор событий и сообщений M^{Q} отдельного ИП или ИР. Это позволяет представить функцию выделения событий и сообщений, обеспечивающих идентификацию состояния отношений агента с отдельным респондентом на уровне отдельного ИП или ИР в виде

$$F^{Q}(m): (\mathrm{QP} \wedge BP) \rightarrow (m \in M_r^{Q}), \; r \in R \quad (9),$$

где *BP* – набор правил $BP = \{b_i, \dots, b_n\}, b_i = \{0,1\}$. Значение «1» для элемента будет означать отнесение отдельного события или сообщения *m* из множества *QP* к набору событий и сообщений, идентифицирующих конкретное состояние отношений агента на уровне ИП и ИР. Таким образом применительно к определению состояния отношения получаем $QP = \bigcup_{r \in R} M_r^{Q}$, при этом $\sum_{r \in R} \left| M_r^{Q} \right| > |QP|$.

В итоге целевая функцию агента с точки зрения категорного подхода должна содержать

$$FT = Ref\left(\psi(m) \circ F^{Q}(m)\right) \circ FM(m) \circ \circ FA(m) \circ F^{\alpha}(m) \quad (10),$$

где:

$F_k = F^{Q}(m) \circ FM(m) \circ FA(m) \circ F^{\alpha}(m)$ – целевая функция отбора событий объекта;

$\psi(*)$ – решающая функция, которая реализует отношение между набором событий и сообщений и состоянием отношений $\psi: M_r^{Q} \rightarrow R$.

Поскольку функции $\psi(m)$ и $F^{Q}(m)$ относятся к отдельным ИП и ИР агента, то необходима также функция *Ref(*),* которая обеспечивает интегральную оценку состояния отношения $\beta R\gamma$ агента с отдельным респондентом на основании исходных данных на уровне ИП или ИР.

Вопросы создания правил и реализации функций указанных в выражениях (5, 6, 7, 9), (применительно к множествам *ME*, *QM, QP)* давно и успешно исследуются [19, 20, см. литературу там же], поэтому в данной статье вопросы реализации указанных выражений рассматривать не будем.

Вместе с тем отметим, что в самом общем виде события и сообщения из состава множества ME и всех его подмножеств:

- Представляют собой алгоритмически определенные семантические структуры, причем для различных ИП и ИР состав и содержание этих структур может значительно различаться.
- В качестве своего источника имеют не только различные ИП и ИР, но и фиксируются (с предварительной обработкой) в нескольких журналах регистрации как в рамках собственно ИП или ИР, так и в рамках агента в целом.
- В процесс реализации целевой функции агента (10) подразумевают внесение изменений структуры и значений содержащейся в событии и сообщении информации.
- Предполагают наличие различных трактовок со стороны различных экспертов как по содержанию, так и по значению событий и сообщений.

Отсюда возникает необходимость в приведении событий и сообщений к единообразному с точки зрения ИБ виду или к их ортогонализации.

Будем использовать общепринятое определение признака как наличие определенных черт, характеристик или свойств дающих основание отнести событие или сообщение к тому или иному типу или классу.

Под ортогонализацией событий и сообщений агента будем понимать формирование единообразных для всех событий и сообщений агента шкал признаков, которые так или иначе содержатся в семантической структуре событий и сообщений. Формирование шкал признаков будем проводить на основе следующего правила:

L1. Признак определяет характер воздействия на носитель данных имеющий определенный уровень последствий

Компоненты этого правила соответствуют следующим морфизмам, определенным во второй части статьи, которые описывают формирование событий и сообщений в агенте.

Компоненте *Характер воздействия* соответствует морфизм $AC \to ME$, описывающий регистрацию действий выполняемых в рамках аккаунта. В соответствии с принятыми в ИБ подходами, компоненте соответствуют операции типа Запись, Чтение, вызывающие изменения Конфиденциальности, Целостности, Доступности для носителя информации. Таким образом можно сформировать шкалу из шести значений для признака *SI* (scale impact).

Компоненте *Носитель данных* соответствует морфизм $Conf \to ME$, описывающий регистрацию фактов выполнения операций с теми или иными носителями данных (включая сюда и программы представленные в виде блоков данных в памяти или на дисках). В современных вычислительных системах, построенных на принципах открытых систем, можно выделить следующие базовые носители данных: Регистры процессора, Оперативная память, Долговременная память, Сетевые адаптеры и Устройства ввода-вывода. Таким образом можно сформировать шкалу из пяти значений для признака *SC* (scale carrier).

Компоненте *Уровень последствий* соответствует морфизм $Prog \to ME$, описывающий статус и режимы выполняемых операций. Поскольку речь идет о событиях и сообщениях, формируемых в агенте как отклик на внешние воздействия, то для перечисления уровней воздействия целесообразно использовать типовые уровни журналирования: fatal, error, warning, info. Таким образом можно сформировать шкалу из четырех значений для признака *SL* (scale level).

Значения шкал признаков можно рассматривать как множества, что дает основание представить любое событие или сообщение как комбинацию значений признаков, то есть как многоместное отношение $SI \times SC \times SL$. Многоместное отношение, описывающее событие или сообщение можно представить в виде схемы признаков $\langle SI, SD, SL \rangle$, поэтому дальше будем использовать только термин «событие». Каждый элемент схемы может содержать наборы значений соответствующих шкал признаков, например, $\{a, b, c\}$, $a, b, c \in SI$ [21, см. литературу там же]. Для демонстрации в дальнейшем необходимых по ходу изложения примеров, определим признаки со следующим составом параметров $SI = \{\theta_1, \theta_2, \theta_3\}$, $SD = \{\lambda_1, \lambda_2, \lambda_3\}$, $SL = \{\mu_1, \mu_2, \mu_3\}$. Равномощность множеств носит исключительно демонстрационный характер.

Необходимо отметить, что согласно правилу *L1*, для каждой операции всегда есть носитель и уровень воздействия, то есть $SI \wedge SD \wedge SL$. Следовательно, выполнение правила *L1*, влечет необходимость выполнения еще двух правил, обеспечивающих полноту описания события и порядок перечисления значений признаков.

L2. Любое событие или сообщение должно соответствовать схеме

$$\exists m: \langle SI, SD, SL \rangle \Rightarrow \exists(\theta_i \in SI) \wedge \exists(\lambda_i \in SD) \wedge \exists(\mu_i \in SL)$$

L3. Порядок перечисления значений признаков при описании события определяется по шкале SI

$$\forall m: \langle SI, SD, SL \rangle, \theta_i \in SI, \lambda_j \in SD, \mu_n \in SL \Rightarrow$$
$$\Rightarrow n = j = i$$

Будем полагать, что шкалы признаков имеют преимущественно качественные значения. В дальнейшем значения шкал признаков будем определять как «параметры». Для соответствия признаков целевой функции (10) применяется следующее условие.

Y4. Число шкал признаков и число параметров для каждой шкалы могут быть различными, но должны быть конечными.

Экспертно формируемые признаки и параметры должны быть единообразны для всех событий объекта. Правило *L1*, и условие *Y4* подразумевают (на основании положений алгебры кортежей) возможность описания одного и того же события несколькими параметрами для каждого из признаков. Например, можно получить кортеж вида

$$m = \langle \{\theta_1, \theta_2\}\{\lambda_3\}\{\mu_1, \mu_3\} \rangle \quad (11)$$

Здесь и далее указание, что конкретные переменные в приводимых выражениях даны для примера, даваться не будет. Отметим, что выражение (11) эквивалентно следующим сочетаниям параметров: $(\theta_1\lambda_3\mu_1)$, $(\theta_1\lambda_3\mu_3)$, $(\theta_2\lambda_2\mu_1)$, $(\theta_2\lambda_3\mu_3)$. Аналогичным (11) образом может быть представлен и некоторый набор событий.

Но представляется очевидным, что подобное определение для наборов событий является недостоверным в силу неизбежного наличия в этом случае ошибочных комбинаций параметров признаков. Например, при рассмотрении кортежа (11) как набора событий, возникающее в процессе его разложения сочетание параметров для отдельного события $m_i = (\theta_2\lambda_3\mu_3)$ может соответствовать несуществующему событию.

Если учесть, что множество событий как агента в целом, так и отдельных ИП или ИР алгоритмически предопределено разработчиками, а наборы правил являются в общем случае результатом экспертных заключений, то выражение (9) позволяет двояко трактовать множество M_r^Q. С одной стороны, для полного набора событий заданного для ИП или ИР, множество M_r^Q представляет из себя эталонные наборы S^r событий для каждого из возможных состояний отношений агента. С другой стороны, регистрируемый в процессе функционирования ИП и ИР набор событий будет отличаться от эталонного набора, который обозначим как текущий набор M^C.

Понятия эталонного и текущего наборов событий также можно описать с помощью предикатов «Событие входит в правило» – $Pr1(m)$, «Событие произошло» – $Pr2(m)$ и «Событие зарегистрировано» – $Pr3(m)$. Эталонный набор событий должен определяться только тавтологией $Pr1(m) \wedge Pr2(m) \wedge Pr3(m)$, в то время как текущий набор событий может быть представлен следующим образом:

$Pr1(m) \wedge Pr2(m) \wedge Pr3(m)$ – событие произошло и зарегистрировано,

$Pr1(m) \wedge Pr2(m) \wedge \overline{Pr3(m)}$ – событие произошло, но не зарегистрировано,

$Pr1(m) \wedge \overline{Pr2(m)} \wedge Pr3(m)$ – событие не произошло, но есть регистрация,

$Pr1(m) \wedge \overline{Pr2(m)} \wedge \overline{Pr3(m)}$ – событие не произошло и не зарегистрировано.

Данные высказывания позволяют говорить, что $M_r^Q \Leftrightarrow S^r \vee M^C$, при этом в силу истинности $Pr1(m)$ во всех высказываниях, на данном этапе исследования можно полагать $|S^r| \geq |M^C|$.

Свертка событий и сообщений

Проведенная в предыдущем разделе ортогонализация событий и сообщений для ИП и ИР агента позволяют упростить терминологию следующим образом: «события и сообщения» далее будем именовать как «события», эталонные наборы событий как «шаблоны», а ИП и ИР, рассматривая их как носители сообщений – как «объекты». Соответственно, введем следующие обозначения:

K – множество объектов в составе агента и $k \in K$ – отдельный объект;

R_k – множество возможных состояния объекта $R_k \subseteq R$ и $r_k \subseteq R_k$ – текущее состояния объекта;

M_k – полный набор событий алгоритмически реализованный на объекте;

F_k – целевая функция отбора событий объекта, как следует из (10);

S_k^r – формируемый экспертно для каждого состояния $r \in R$ и для каждого объекта $k \in K$ шаблон событий, $S_k^r \subseteq M_k$;

C_k – текущий набор событий отдельного объекта $k \in K$, формируемый алгоритмически на дискретный момент времени, $C_k \subseteq M_k$;

$V_k^r = \{S_k^r | r \in R, k = const\}$, $V_k^r \subseteq M_k$ – вариант, когда отдельное состояние объекта (или группы объектов) описывается несколькими шаблонами событий.

Также сформулируем дополнительные условия.

Y5. Одно и тоже событие может входить в разные шаблоны для разных состояний $\sum_{k \in K} |S_k^r| \geq |M_k|$.

Y6. Для каждого состояния и для каждого объекта существует не менее одного шаблона событий $\forall r \forall k \; \exists S_k^r$.

Отметим, что шаблоны состояний S_k^r для каждого объекта относительно постоянны: они могут изменяться только при внесении разработчиками изменений в их состав. В то время как расчеты состояний объекта выполняются в дискретные моменты времени. Вопросы формирования текущих наборов и влияние дискретов времени на оценку состояния отношений требуют отдельного исследования.

Сделаем следующее утверждение

Утверждение 1. Состояние объекта определяется соотнесением текущего набора событий и эталонного набора $r_k = \varphi(C_k, S_k^r)$.

Доказательство будем проводить по необходимости и достаточности.

Необходимость. Если представлять взаимосвязи между состоянием r_k, формулой F_k и шаблоном S_k^r с точки зрения необходимости, то получим следующее правило. Для определения состояния необходима формула, а для расчета формулы необходим соответствующий шаблон событий. Что через отношение необходимости можно записать как $(r_k \leftarrow F_k) \wedge (F_k \leftarrow S_k^r)$. В силу правила цепного заключения получаем формулирование состояния на основе эталонного набора событий $r_k \leftarrow S_k^r$.

Достаточность. Если представлять взаимосвязи между состоянием r_k, формулой F_k и текущим набором C_k с точки зрения достаточности, то получим следующее правило. Из заданности r_k и F_k следует, что для определения текущего состояния достаточно формулы, а для расчета формулы достаточно соответствующего набора событий. Что через отношение достаточности можно записать как $(C_k \rightarrow F_k) \wedge (F_k \rightarrow r_k)$. Опять же в силу правила цепного заключения имеем определение состояния на основе текущего набора событий $C_k \rightarrow r_k$.

В итоге получаем $C_k \rightarrow r_k \leftarrow S_k^r$. С точки зрения теории категорий, речь можно вести о коммутационной диаграмме уравнителя, изображенной на рисунке 1.

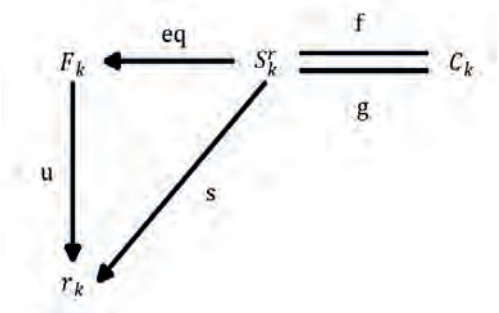

Рис. 1. Коммутационная диаграмма уравнителя

Морфизм *eq* следует из (10). Морфизм *m* следует из *Y6*. На основании этих же условий можно записать $r_k = F_k(M_k)$, что определяет морфизм *u*. При этом вследствие условий необходимости и достаточности выполняется требование $eq \circ u = s$ для уравнителя. В результате получаем $f \circ s = g \circ s$. Следовательно, подлежащим определению остается именно результат соотнесения текущего и эталонного наборов событий. Что и требовалось доказать.

Назовем функцию $\varphi(C_k, S_k^r)$ функцией вхождения. Как следует из диаграммы рисунка 1, результатом работы функция вхождения фактически является двоичный вектор, формируемый по следующему правилу

$$\varphi(x, y) = \begin{cases} 1, \exists (f \vee g) \\ 0, \nexists (f \vee g) \end{cases} \quad (12)$$

где: $x \in C_k$ и $y \in S_k^r$.

Морфизмы *f* и *g* на рисунке 1 можно трактовать с точки зрения направления сравнения текущего и эталонного наборов событий в зависимости от их мощности. Если состав эталонного набора событий по смыслу формируется разработчиком объекта , то состав текущего набора событий полностью зависит от дискретов времени в течение которого он формируется. Как уже отмечалось ранее, вопрос зависимости результатов сравнения наборов событий от дискретов времени заслуживает отдельного исследования.

Таким образом, в следствие *Утверждения 1*, задачу определения состояния объекта агента по текущему набору событий следует рассматривать как определения факта наличия совпадения (12) текущего набора событий со всеми возможными для данного объекта и данного состояния шаблонами, то есть вариантами.

$$\varphi(C_k, S_k^r) : C_k \bigcap\nolimits_{r \in R} V_k^r \neq \emptyset \quad (13)$$

Наличие морфизмов *f* и *g* на рисунке 1 кроме того является причиной возможного комбинаторного взрыва, поскольку показывает необходимость проведения сравнения событий текущего и эталонных наборов по принципу «каждый с каждым».

Но с учетом условия *Y4* и правила *L2* (как было показано на примере (11)), каждое событие представляет из себя однозначно *определенное* сочетание строго *определенных* морфизмов между множествами параметров именно *различных* признаков. Что дает основание сделать следующее утверждение.

Утверждение 2. Параметры признаков могут использоваться как обозначения координат морфизмов.

Доказательство основано на определении морфизма $f: X \rightarrow Y$, где именование начала и окончание морфизма как ребра направленного графа $dom(f) = X$ и $cod(f) = Y$. Правила *L1* и *L2* и пример (11) позволяют рассматривать собы-

тие как многоместное отношение между признаками с морфизмами $f: SI \to SD$ и $g: SD \to SL$, то есть для f – $dom(f) = SI$, $cod(f) = SD$ и для g – $dom(g) = SD$, $cod(g) = SL$. Следовательно, можем представить событие как $m \Leftrightarrow g(\theta,\lambda) \bowtie f(\lambda,\psi)$, где через $\bowtie$ обозначим сцепку морфизмов для соответствующих параметров признаков. Введение операции сцепки определяется в общем случае необходимостью соблюдения порядка следования признаков, определяемого правилом *L1*. Соответственно, все возможные сочетания морфизмов по признакам для объекта можно записать как $M_k = Hom(SI, SD) \times Hom(SD, SL)$. Обозначим через $H = \sum_{r \in R} |S_k^r|$ общее число всех событий, образующих шаблоны всех состояний объекта, а сочетания морфизмов для таких событий, как $W_k = \bigcup_{i \in H} (g_i(\theta,\lambda) \bowtie f_i(\lambda,\psi))$. Тогда в соответствии с коммутационной диаграммой классификатора представленной на рисунке 2, морфизм $M_k \to \{0,1\}$ представляет собой характеристическую функцию, принимающую значение 1 на подмножестве W_k, что дает основания говорить о вытекающей из (10) функции отбора F_k.

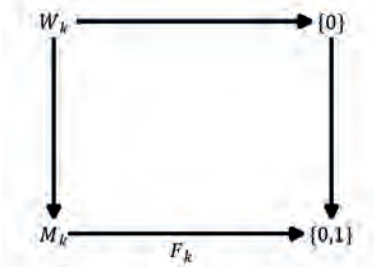

Рис. 2. Коммутационная диаграмма классификатора

Таким образом, F_k есть функция отбора событий для формирования шаблонов состояний объекта именно на основе сцепки морфизмов $g(\theta,\lambda) \bowtie f(\lambda,\psi)$. Доказательство закончено.

По индукции любой набор событий объекта для отдельного состояния при произвольном, но конечном числе признаков (например, $\{A, \cdots, Z\}$) может быть представлен как

$$M_k, C_k, S_k^r, V_k^r \Leftrightarrow Hom(A,B) \times_{F_k} \cdots \quad (14)$$
$$\cdots \times_{F_k} Hom(Y,Z)$$

Утверждение 3. Параметр первого признака в схеме события может использоваться для именования сцепки морфизмов соответствующей определенному событию.

Доказательство. Доказательство будем проводить используя обозначения принятые в примере (11). Пусть $\mathbf{A}$ – множество шкал признаков, $\mathbf{B}$ – это произведение $SD \times_A SL$ над $\mathbf{A}$ вместе с морфизмами $b_1: SD \to \lambda_m$ и $b_2: SL \to \mu_m$ определяющими параметры для конкретного события m. Морфизмы a_1 и a_2 дают декартов квадрат такой, что $B = \{(\lambda_m, \mu_m) \in SD \times SL: a_1(\lambda_m) = a_2(\mu_m)\}$.

То есть, морфизмы a_1 и a_2 определяют выбор конкретных параметров признаков. Далее, в силу правила *L2* и выражения (11), мы можем ввести шкалу признака SI и морфизмы $q_1: SI \to SD$ и $q_2: SI \to SL$ сохраняя коммутативность диаграммы как показано на рисунке 3.

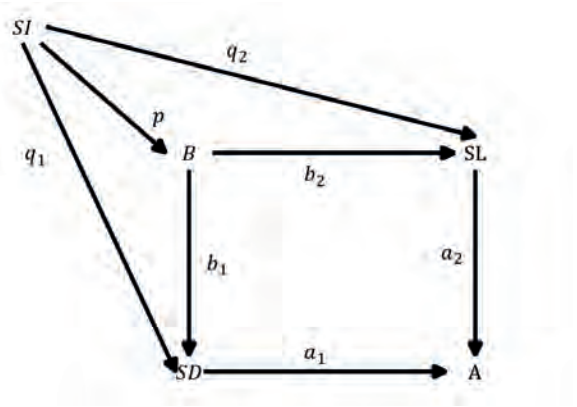

Рис. 3. Коммутативная диаграмма именования

Соответственно, имеет место единственный морфизм $p: SI \to B$, который и является именованием сцепки морфизмов, соответствующих определенному событию, что и требовалось доказать. Доказательство утверждения 3 для числа признаков больше трех проводится по индукции.

Приведенные рассуждения позволяют сконструировать свертку событий в виде матрицы, где:

- строки поименованы параметрами шкалы SD,
- столбцы поименованы параметрами шкалы SL,
- ячейки матрицы содержат параметры шкалы SI для каждого события в свертке.

При этом:

- согласно правилу *L1*, для каждой операции всегда есть носитель и уровень воздействия, то есть отношения между признаками сюрьективны $SI \mapsto SD \mapsto SL$, что влечет за собой их упорядоченность;
- порядок следования параметров признаков по столбцам и строкам матрицы может быть произвольный, но фиксированный все время применения свертки;
- для функции вхождения порядок следования событий может быть произвольным.

Применение свертки событий

Пример 1. Примерный вид матрицы в соответствии с приведенным ранее примером (11) как набора событий и исключением из него $m_i = (\theta_2 \lambda_3 \mu_3)$ через параметры признаков приведен ниже.

	λ_1	λ_2	λ_3
μ_1			θ_2, θ_1
μ_2			
μ_3			θ_1

Пример 2. Пусть набор событий состоит из $m_1 = (\theta_1 \lambda_1 \mu_1)$ $m_2 = (\theta_2 \lambda_2 \mu_2)$ $m_3 = (\theta_3 \lambda_3 \mu_3)$. Кортеж набора имеет вид $\langle\{\theta_1, \theta_2, \theta_3\}\{\lambda_1, \lambda_2, \lambda_3\}\{\mu_1, \mu_2, \mu_3\}\rangle$ и при его разложении даст ложные определения событий. В то время как матрица таких ошибок не дает

	λ_1	λ_2	λ_3
μ_1	θ_1		
μ_2		θ_2	
μ_3			θ_3

Пример 3. Пусть набор событий состоит из $m_1 = (\theta_1 \lambda_1 \mu_1)$ $m_2 = (\theta_2 \lambda_2 \mu_2)$ $m_3 = (\theta_3 \lambda_3 \mu_3)$ $m_4 = (\theta_2 \lambda_1 \mu_1)$. Кортеж набора имеет вид $\langle\{\theta_1, \theta_2, \theta_3\}\{\lambda_1, \lambda_2, \lambda_3\}\{\mu_1, \mu_2, \mu_3\}\rangle$ при его разложении даст ложные определения событий. Матрица свертки для такого набора событий имеет вид

	λ_1	λ_2	λ_3
μ_1	θ_1, θ_2		
μ_2		θ_2	
μ_3			θ_3

Использование матрицы свертки событий рассмотрим на следующем примере.

Пример 4. Пусть отдельное состояние объекта описывается вариантом из двух шаблонов событий, которые образуют С-систему алгебры кортежей, являющуюся аналогом ДНФ системы.

$$A1 = \begin{bmatrix} \{a,b\} & \{f,e\} & \{g,h\} \\ \{a,c\} & \{d,e\} & \{h,j\} \end{bmatrix}$$

Отметим, что для такого представления варианта состояния объекта, события должны быть упорядочены по их источникам, то есть иметь схему $\langle Log1 Log2 Log3\rangle$. Пусть также задан текущий набор событий $A2 = [\{b,c\} \quad \{d,f\} \quad \{g,j\}]$. Алгебра кортежей позволяет выполнить операцию проверки включения кортежа *A2* в систему *A1*, что соответствует определению функции вхождения (13). В общем виде проверка включения основана на разбиении A1 и A2 на элементарные кортежи вида $A1' = \{(afg), \cdots, (beh), (adh), \cdots, (cej)\}$ и $A2' = \{(bdg), \cdots, (cfj)\}$ и их попарном пересечении $A2' \cap A1' = (bdg) \cap (afg), \cdots, (cfj) \cap (beh), (bdg) \cap (adh), \cdots, (cfj) \cap (cej)$

Результат проверки включения требует дальнейшей интерпретации, но представляет интерес определение числа операций пересечения, поскольку алгебра кортежей представляется общепризнанным инструментом работы с множествами. Данное число можно определить как $\sum_{i \in v}(|A2'| \times |A_i'|)$, где *v* – число наборов в варианте шаблонов *A1*, то есть речь идет о полиноминальной зависимости от размеров текущего и эталонного наборов событий. Разработанные алгоритмы снижения числа пересечений не отменяют полиноминальной зависимости от размерности.

При использовании матрицы свертки событий справедливо следующее утверждение.

Утверждение 4. Проверка вхождения текущего набора событий в эталонный имеет линейный характер зависимости от размерности сравниваемых компонент.

Доказательство. При использовании для определения состояния отношения объекта матрицы свертки, С-система А1 представляет из себя матрицу эталонного набора событий, а кортеж А2 – множество событий текущего набора.

Построение матрицы свертки проводится аналогично предыдущим примерам и рассматриваться не будет. Отметим только, что в ее основе лежит схема размерности $SI = \{\theta_1, \theta_2, \theta_3, \theta_4, \theta_5, \theta_6\}$, $SD = \{\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5\}$, $SL = \{\mu_1, \mu_2, \mu_3, \mu_4\}$, что дает возможность классифицировать события с точки зрения ИБ по 120 типам.

В соответствии с определением события $m_i = (\theta_i \lambda_i \mu_i)$, примем λ_i и μ_i в качестве координат текущего или эталонного события, а θ_i – как сравниваемые величины. Обозначим координаты матрицы свертки *A1* (наименование строк и столбцов) как λ_i и μ_i а для каждого события из *A2* как λ_i', μ_i'. соответственно. Координаты текущего и эталонного событий идентичны, поскольку являются *i-м* элементом множеств SD и SL с одинаковым индексом. Следовательно, применение λ_i', μ_i' текущего события к матрице свертки дает содержимое соответствующей ячейки матрицы.

Введем функции:

— ρ (m), возвращающую координаты конкретного события $(x, y) = \rho(m)$;

— $\pi(\rho(m),A1)$, возвращающую содержимое ячейки матрицы $\Theta_{x,y} = \pi((x, y), A1)$.

Будем полагать, что величина θ_i' получается автоматически из определения события. В итоге получаем выражение, дающее подмножество содержащее $\emptyset$ или θ_i' для событий текущего набора $m_i' \in A2 \Rightarrow z_i = \theta_i' \cap \Theta_{x,y}$

Тогда, при начальном значении $Z = \emptyset$ выражение (13) можно записать как

$$\varphi(C_k, S_k^r): \forall m_i \in C_k, Z \coprod_{i \in |C_k|} (z_i, i) \mid z_i \neq \emptyset \quad (15)$$

Анализ выражения (15) с учетом определения функции $\pi(\rho(m),A1)$ показывает, что количество операций, необходимых для получения результата вхождения C_k в S_k^r линейно зависит от размера текущего набора событий. Что и требовалось доказать.

Получаемое в результате вычисления $Z = \varphi(C_k, S_k^r)$ множество позволяет определить количественные характеристики вхождения C_k в S_k^r:

— мощность множества Z характеризует уровень совпадения текущего и эталонного наборов событий;

— набор параметров θ из C_k, позволяющий при необходимости ввести дополнительные оценки совпадения текущего и эталонного наборов событий с точки зрения конфиденциальности, целостности и доступности.

Положим, что матрица свертки событий создана для всех возможных вариантов состояний отношений. Тогда решающая функция $\psi: M_r^Q \to R$ из (10) может быть определена следующим образом $M_r^Q = \{C_k, V_k^1, \cdots, V_k^n\}$, где $n = |R|$. С учетом (15) получаем результат работы решающей функции $Q_k = \forall r \in R \ \varphi(C_k, V_k^r) = [Z_k^1, \cdots, Z_k^n]$ – вектор оценок каждого из состояний для конкретного объекта.

Функцию определения интегральной оценки состояния отношения $\beta R \gamma$ агента с отдельным респондентом на основании исходных данных на уровне ИП или ИР $Ref(Q_k)$ рассмотрим в следующей статье цикла.

Типизация агента

Из выражения (4) и последующих рассуждений, дающих выражения (5) – (10), можно положить, что в самом общем виде состояние агента можно рассматривать с двух точек зрения: что он знает о себе (внутренняя оценка) и что агент знает о своем окружении (внешняя оценка). Соответственно, множество *ME* может быть разделено на следующие целевые подмножества: M^β – события и сообщения доступные агенту и M^γ – события и сообщения доступные респонденту.

Представление агента в виде автомата (2) позволяет представить эти подмножества в следующем виде: $M^\beta = \{MS^\beta, QM_\gamma, MS^\gamma\}$ и $M^\gamma = \{MS^\gamma, MS^\beta, QM_\gamma\}$

Напомним, что QM_γ – алгоритмически определенный по составу и содержанию конечный набор событий и сообщений, определяющий реакцию агента на внешние воздействия, MS^β – исходящие сообщения агента, MS^γ – входящие сообщения агента

Результаты предыдущих разделов статьи позволяют доопределить функции автомата (2) следующим образом: функция воздействия $\delta: MS^\gamma \to QM_\gamma$ и функция отклика $\pi: QM_\gamma \to MS^\beta$. То есть, множества M^β и M^γ следует рассматривать как видимость результатов работы функций воздействия и отклика. Представляется целесообразным под видимостью понимать мощность множеств MS^γ, MS^β, QM_γ доступных со стороны агента и респондента. Для этого введем функцию видимости $F^*: |X| \xrightarrow{\Omega} |Y|$, осуществляющую фильтрацию множеств MS^γ, MS^β, QM_γ в M^β и M^γ.

Тогда должно выполняться условие $|Y| \leq |X|$, что соответствует выражению $|Y| = |X|/\Omega$. Аналогично с M^β и M^γ функции видимости будем обозначать как $F^\beta(X, \Omega)$ и $F^\gamma(X, \Omega)$.

Определения и выводы первой части статьи позволяют представить Защитника и Нарушителя в качестве агентов. Положим, что респондентом является Нарушитель (*H*), а агентом - Защитник (*D*). Отсюда следует, что множества M^β и M^γ и соответствующие функции видимости имеют двойственную природу: каждый из субъектов (представленный как агент) воспринимает другую сторону взаимодействия как респондента. Для уточнения принадлежности функций введем следующие обозначения:

$F^\beta\lfloor_D(*)$ – функция обеспечивающая видимость сообщений Защитником своих собственных сообщений;

$F^\gamma\lfloor_D(*)$ – функция обеспечивающая видимость сообщений Защитника со стороны Нарушителя;

$F^\gamma\lfloor_H(*)$ – функция обеспечивающая видимость сообщений Нарушителя со стороны Защитника;

$F^\beta\lfloor_H(*)$ – функция обеспечивающая видимость сообщений Нарушителем своих собственных сообщений.

Тогда базовые действия Защитника, применимые для всех агентов из состава ИС, можно сформулировать следующим образом

$$SA_{QM}(D) = \arg\max_{\Omega} F^{\beta}\lfloor_{D}(QM_{\gamma},\Omega) \wedge \wedge \arg\min_{\Omega} F^{\gamma}\lfloor_{D}(QM_{\gamma},\Omega) \quad (16)$$

Выражение (16) означает наибольшую видимость внутренних сообщений агента со стороны Защитника и наименьшую видимость таких сообщений для Нарушителя.

$$SA_{MS^{\beta}}(D) = \arg\min_{\Omega} F^{\gamma}\lfloor_{D}(MS^{\beta},\Omega) \quad (17)$$

Выражение (17) означает минимизацию для Нарушителя видимости исходящих сообщений Защитника или иначе – ограничение для Нарушителя возможности видеть результаты его деятельности.

$$SA_{MS^{\gamma}}(D) = \arg\min_{\Omega} F^{\gamma}\lfloor_{D}(MS^{\gamma},\Omega) \quad (18)$$

Выражение (18) означает минимизацию видимости со стороны Нарушителя входящих сообщений Защитника или иначе – ограничение возможности Нарушителя воздействовать на Защитника.

В целом, на основании (16) – (18) действия Защитника могут быть сформулированы как $SA(D) = SA_{QM}(D) \wedge SA_{MS^{\beta}}(D) \wedge SA_{MS^{\gamma}}(D)$, что соответствует стремлению Защитника иметь возможно более полную информацию о состоянии ИП и ИР агента, а также в наибольшей степени ограничить возможности Нарушителя по получению такой информации и воздействию на ИП и ИР агента.

Для Нарушителя базовые действия формулируются аналогично.

$$SA_{QM}(H) = \arg\max_{\Omega} F^{\gamma}\lfloor_{D}(QM_{\gamma},\Omega) \wedge \wedge \arg\max_{\Omega} F^{\beta}\lfloor_{H}(QM_{\gamma},\Omega) \wedge \wedge \arg\min_{\Omega} F^{\gamma}\lfloor_{H}(QM_{\gamma},\Omega) \quad (19)$$

Выражение (19) означает стремление Нарушителя обеспечить наибольшую видимость внутренних сообщений своего агента и атакуемого респондента (Защитника) и в то же время обеспечить наименьшую видимость своих сообщений для Защитника или иначе – максимально скрыть от Защитника свою деятельность.

$$SA_{MS^{\beta}}(H) = \arg\max_{\Omega} F^{\beta}\lfloor_{H}(MS^{\beta},\Omega) \wedge \wedge \arg\min_{\Omega} F^{\gamma}\lfloor_{H}(MS^{\beta},\Omega) \quad (20)$$

Выражение (20) означает стремление обеспечить наибольшую видимость своих исходящих сообщений со стороны Нарушителя и минимизировать их видимость для Защитника или иначе – максимально скрыть свои атакующие действия.

$$SA_{MS^{\gamma}}(H) = \arg\max_{\Omega} F^{\beta}\lfloor_{H}(MS^{\gamma},\Omega) \wedge \wedge \arg\min_{\Omega} F^{\gamma}\lfloor_{H}(MS^{\gamma},\Omega) \quad (21)$$

Выражение (21) означает стремление Нарушителя иметь максимальную видимость для входящих сообщений от Защитника и при этом обеспечить их минимальную видимость для Защитника или иначе – скрыть свою осведомленность.

В целом, на основании (19) – (21) действия Нарушителя могут быть сформулированы как $SA(H) = SA_{QM}(H) \wedge SA_{MS^{\beta}}(H) \wedge SA_{MS^{\gamma}}(H)$, что соответствует стремлению Нарушителя иметь максимально полную информацию о состоянии ИП и ИР респондента (атакуемого агента) и возможность воздействовать на них, а также в наибольшей степени скрыть события и сообщения описывающие его действия с ИП и ИР респондента.

В качестве промежуточного итога отметим.

1. Защитник не может ограничить действие $lim(SA_{MS^{\gamma}}(D)) \to 0$ и $lim(SA_{MS^{\beta}}(D)) \to 0$ в силу необходимости обеспечения доступности ИР и ИП агента, что означает невозможность исключения деструктивных действий Нарушителя.в отношении агента.

2. В выражении (16) присутствует требование $F^{\beta}(QM_{\gamma},\Omega) > F^{\gamma}(QM_{\gamma},\Omega)$, а в выражении (19) присутствует требование $F^{\gamma}(QM_{\gamma},\Omega) > F^{\beta}(QM_{\gamma},\Omega)$, что дает противоречие в требованиях к функционированию агента и входящих в его состав объектов.

Представляется принципиально важным отметить следующие особенности, которые обозначим как исходные посылки.

P1. Определение состояния объекта из состава агента не зависит от принадлежности аккаунта данного агента Защитнику или Нарушителю.

P2. Определение состояния объекта из состава агента основывается на алгоритмически заданных событиях, которые не могут быть изменены в процессе функционирования агента.

P3. Для Защитника и Нарушителя, представленных в виде аккаунта агента, базовые действия эквивалентны.

P4. Определение базовых действия основывается на тех же алгоритмически заданных событиях объектов.

P5. Отличие между базовыми действиями и определением состояния заключается в способах фильтрации событий объекта.

P6. Защитник не может ограничить действие $lim(SA_{MS^{\gamma}}(D)) \to 0$ и $lim(SA_{MS^{\beta}}(D)) \to 0$ в силу необходимости обеспечения доступности ИР и ИП агента, что означает невозможность исключения деструктивных действий Нарушителя.в отношении агента.

P7. В выражении (16) присутствует требование $F^{\beta}(QM_{\gamma},\Omega) > F^{\gamma}(QM_{\gamma},\Omega)$, а в выражении (19) присутствует требование $F^{\gamma}(QM_{\gamma},\Omega) > F^{\beta}(QM_{\gamma},\Omega)$, что дает противоречие в требованиях к функциониро-

ванию агента и входящих в его состав объектов

Посылки *P1-P7* дают основание выдвинуть следующую гипотезу.

Объекты из состава агента и агент в целом, осуществляющие обработку информации в интересах Пользователя, имманентно не обладают способностью обеспечить конфиденциальность, целостность и доступность информации. В случае получения Нарушителем аккаунта агента, все объекты агента неизбежно становятся инструментом Нарушителя.

В терминах теории категорий можно также выдвинуть «*ко*-»гипотезу.

Защиту информации в информационной системе можно обеспечить только за счет наличия и топографии размещения специализированных агентов, которые на любое внешнее воздействие респондентов, связанное с обработкой информации в интересах Пользователя, обеспечивают состояние отношений «Безразличное», когда агент целенаправленно не участвует в процессах обработки информации респондентами, но при этом обладает способностью влиять на информационные потоки взаимодействия респондентов.

Следует отметить, что современные технологии построения информационных систем, такие как виртуализация, микросервисы и инфраструктура как код, может быть впервые за всю историю развития вычислительной техники, дают возможность реализации таких агентов. Главным качеством таких агентов будет их построение на основе принципа отсутствия физических и логических адресов на всех интерфейсах, кроме управляющего. Такие возможности предоставляют технологии типа «ethernet-bridge», успешным примером практической реализации которых является, например, изделии ССПТ-2 НПО «Фрактел».

Заключение

Результаты исследования и разработок данной статьи дают возможность определять состояние отношений информационных потоков и информационных ресурсов из состава агента с его респондентами на основе матрицы сверток событий, что позволяет:

- Обеспечить линейную зависимость операций проверки вхождения текущего набора событий в эталонный только от размерности текущего набора.
- Обеспечить возможность параллельного и независимого определения состояния отношений для разных объектов.
- Обеспечить предварительное формирование на этапе разработки правил отбора, ортогонализации, формирования эталонных наборов и матриц свертки событий, что позволит значительно ускорить определение состояния отношений в процессе работы агента.

Целесообразно обеспечить формирование правил отбора, ортогонализации, формирования эталонных наборов и матриц свертки событий разработчиками ИП и ИР в рамках выполнения нормативных требований по ИБ (например, в рамках выполнения ГОСТ ИСО/МЭК 15408).

Кроме того, в рамках ортогонализации событий, целесообразно обеспечить выработку экспертным сообществом признаков и параметров ортогонализации и внесение соответствующих изменений в состав и способы регистрации событий информационных ресурсов и информационных потоков агентов.

Литература

1. Рябинин, И.А. Решение одной задачи оценки надежности структурно-сложной системы разными логико-вероятностными методами / И.А. Рябинин, А.В. Струков // Моделирование и анализ безопасности и риска в сложных системах, Санкт-Петербург, 19–21 июня 2019 года. – Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2019. – С. 159-172.
2. Демин, А.В. Глубокое обучение адаптивных систем управления на основе логико-вероятностного подхода / А.В. Демин // Известия Иркутского государственного университета. Серия: Математика. – 2021. – Т. 38. – С. 65-83. – DOI 10.26516/1997-7670.2021.38.65
3. Викторова, В.С. Вычисление показателей надежности в немонотонных логико-вероятностных моделях многоуровневых систем / В.С. Викторова, А.С. Степанянц // Автоматика и телемеханика. – 2021. – № 5. – С. 106-123. – DOI 10.31857/S000523102105007X.
4. Леонтьев, А.С. Математические модели оценки показателей надежности для исследования вероятностно-временных характеристик многомашинных комплексов с учетом отказов / А.С. Леонтьев, М.С. Тимошкин // Международный научно-исследовательский журнал. – 2023. – № 1(127). С. 1 – 13. – DOI 10.23670/IRJ.2023.127.27.
5. Пучкова, Ф.Ю. Логико-вероятностный метод и его практическое использование / Ф.Ю. Пучкова // Информационные технологии в процессе подготовки современного специалиста: Межвузовский сборник научных трудов / Министерство просвещения Российской Федерации; Федеральное государственное бюджетное образовательное учреждение высшего образования «Липецкий

государственный педагогический университет имени П.П. Семенова-Тян-Шанского». Том Выпуск 25. – Липецк: Липецкий государственный педагогический университет имени П.П. Семенова-Тян-Шанского, 2021. – С. 187-193.
6. Россихина, Л.В. О применении логико-вероятностного метода И.А. Рябинина для анализа рисков информационной безопасности / Л.В. Россихина, О.О. Губенко, М.А. Черноситова // Актуальные проблемы деятельности подразделений УИС: Сборник материалов Всероссийской научно-практической конференции, Воронеж, 20 октября 2022 года. – Воронеж: Издательско-полиграфический центр «Научная книга», 2022. – С. 108-109.
7. Карпов, А.В. Модель канала утечки информации на объекте информатизации / А.В. Карпов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах, Санкт-Петербург, 28 февраля – 01 марта 2018 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2018. – С. 378-382.
8. Методика кибернетической устойчивости в условиях воздействия таргетированных кибернетических атак / Д.А. Иванов, М.А. Коцыняк, О.С. Лаута, И.Р. Муртазин // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах, Санкт-Петербург, 28 февраля – 01 марта 2018 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2018. – С. 343-346.
9. Елисеев, Н.И. Оценка уровня защищенности автоматизированных информационных систем юридически значимого электронного документооборота на основе логико-вероятностного метода / Н.И. Елисеев, Д.И. Тали, А.А. 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. Инфраструктура как код: формируется новая реальность информационной безопасности / А.О. Калашников, К.А. Бугайский // Информация и безопасность. – 2019. – Т. 22, № 4. – С. 495-506.
13. Бугайский, К.А. Расширенная модель открытых систем (Часть 1) / К. А. Бугайский, Д. С. Бирин, Б. О. Дерябин, С. О. Цепенда // Информация и безопасность. – 2022. – Т. 25, № 2. – С. 169-178. – DOI 10.36622/VSTU.2022.25.2.001.
14. Калашников А.О. Применение логико-вероятностного метода в информационной безопасности (Часть 1) / Калашников А.О., Бугайский К.А., Бирин Д.С., Дерябин Б.О., Цепенда С.О., Табаков К.В. // Вопросы кибербезопасности. – 2023. – №4(56). – С. 23-32.
15. Калашников А.О. Применение логико-вероятностного метода в информационной безопасности (Часть 2) / Калашников А.О., Бугайский К.А., Аникина Е. И., Перескоков И.С., Петров Ан.О., Петров Ал.О., Храмченкова Е.С., Молотов А.А. // Вопросы кибербезопасности. – 2023. – №5(57). – С. 113–127. DOI:10.21681/2311-3456-2023-6-113-127.
16. Бугайский, К.А. Расширенная модель открытых систем (Часть 2) / К.А. Бугайский, И.С. Перескоков, А.О. Петров, А.О. Петров // Информация и безопасность. – 2022. – Т. 25, № 3. – С. 321-330. – DOI 10.36622/VSTU.2022.25.3.001.
17. Бугайский, К.А. Расширенная модель открытых систем (Часть 3) / К.А. Бугайский, Б.О. Дерябин, К.В. Табаков, Е.С. Храмченкова, С.О. Цепенда // Информация и безопасность. – 2022. – Т. 25, № 4. – С. 501-512.
18. Калашников, А. О. Модель количественного оценивания агента сложной сети в условиях неполной информированности / А. О. Калашников, К. А. Бугайский // Вопросы кибербезопасности. – 2021. – № 6(46). – С. 26–35. – DOI 10.21681/2311-3456-2021-6-26-35.
19. 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. – DOI 10.21681/2311-3456-2017-5-2-16.
20. 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.
21. Кулик, Б. А. Логика и математика: просто о сложных методах логического анализа / Б. А. Кулик. – Санкт-Петербург : Издательство «Политехника», 2021. – 141 с. – ISBN 978-5-7325-1166-6. – DOI 10.25960/7325-1166-6.

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

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

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

Research method: *during the research, the main provisions of the methodology of structural analysis, system analysis, decision theory, category theory, methods for evaluating events under the condition of incomplete information, logical-probabilistic methods 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 from the agent. A scheme of features for representing events from the point of view of information security has been developed and a method for uniform representation of events and messages coming from different sources has been proposed. It is proved that the state of the relationship at the level of an information resource or information flow is determined as a result of the correlation of the current and reference sets of events. It is proved that events and their sets can be represented as multi-place relations of features. It is proved that each feature relation for an event can be named by the first element of the feature scheme. A feature convolution matrix has been developed containing only permitted combinations of feature parameters for sets of events describing the state of relations. It is proved that the application of the convolution matrix gives a linear dependence on the dimension of the sets of events. Formal definitions of the basic actions of the Defender and the Violator on the agent are given. The necessity of making changes to the composition and methods of registering information security events of information resources and information flows is substantiated.*

Scientific novelty: *consideration of information security issues using the apparatus of mathematical and logical relations, as well as category theory. Development of an event convolution matrix based on a categorical approach to determine the state of an agent's relationships. Proof of the linear dependence of the comparison operations of the current and reference sets of events when using the event convolution matrix. Development of formal definitions of basic agent operations for the Defender and the Violator. Two hypotheses describing the agent's capabilities in the field of information security are formulated.*

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

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.

9 Andrey O. Kalashnikov, Dr.Sc. (Technology), Principal Researcher at the Laboratory "Complex networks", Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: aokalash@ipu.ru

10 Konstantin A. Bugajskij, Junior Researcher at the Laboratory "Complex networks", Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E mail: kabuga@ipu.ru

11 Eugenia V. Anikina, Research Fellow, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. E-mail: ajanet@ipu.ru

12 Ilia S. Pereskokov, Junior Researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. E-mail: pereskokov @phystech.edu

13 Andrei O. Pereskokov, Junior Researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. E-mail: petrovaojob@gmail.com

14 Aleksandr O. Petrov – Junior Researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. E-mail: petrovalexandr@ipu.ru

15 Khramchenkova E.S.– Junior Researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. E-mail: hramchenkovaes@yandex.ru

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

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.
7. Karpov, A.V. Model' kanala utechki informacii na ob"ekte informatizacii / A.V. Karpov // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO 2018): VII Mezhdunarodnaya nauchno-tekhnicheskaya i nauchno-metodicheskaya konferenciya. Sbornik nauchnyh statej. V 4-h tomah, Sankt-Peterburg, 28 fevralya – 01 marta 2018 goda / Pod redakciej S.V. Bachevskogo. Tom 2. – Sankt-Peterburg: Sankt-Peterburgskij gosudarstvennyj universitet telekommunikacij im. prof. M.A. Bonch-Bruevicha, 2018. – pp. 378-382.
8. Metodika kiberneticheskoj ustojchivosti v usloviyah vozdejstviya targetirovannyh kiberneticheskih atak / D.A. Ivanov, M.A. Kocynyak, O.S. Lauta, I.R. Murtazin // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO 2018): VII Mezhdunarodnaya nauchno-tekhnicheskaya i nauchno-metodicheskaya konferenciya. Sbornik nauchnyh statej. V 4-h tomah, Sankt-Peterburg, 28 fevralya – 01 marta 2018 goda / Pod redakciej S.V. Bachevskogo. Tom 2. – Sankt-Peterburg: Sankt-Peterburgskij gosudarstvennyj universitet telekommunikacij im. prof. M.A. Bonch-Bruevicha, 2018. – pp. 343-346.
9. Eliseev, N.I. Ocenka urovnya zashchishchennosti avtomatizirovannyh informacionnyh sistem yuridicheski znachimogo elektronnogo dokumentooborota na osnove logiko-veroyatnostnogo metoda / N.I. Eliseev, D.I. Tali, A.A. Oblanenko // Voprosy kiberbezopasnosti. – 2019. – № 6(34). – pp. 7-16. – DOI 10.21681/2311-3456-2019-6-07-16.
10. Kocynyak, M.A. Matematicheskaya model' targetirovannoj komp'yuternoj ataki / M.A. Kocynyak, O.S. Lauta, D.A. Ivanov // Naukoemkie tekhnologii v kosmicheskih issledovaniyah Zemli. – 2019. – T. 11, № 2. – pp. 73-81. – DOI 10.24411/2409-5419-2018-10261.
11. Belyakova, T.V. Funkcional'naya model' processa vozdejstviya celevoj komp'yuternoj ataki / T.V. Belyakova, N.V. Sidorov, M.A. Gudkov // Radiolokaciya, navigaciya, svyaz': Sbornik trudov XXV Mezhdunarodnoj nauchno-tekhnicheskoj konferencii, posvyashchennoj 160-letiyu so dnya rozhdeniya A.S. Popova. V 6-ti tomah, Voronezh, 16–18 aprelya 2019 goda. Tom 2. – Voronezh: Voronezhskij gosudarstvennyj universitet, 2019. – pp. 108-111.
12. Kalashnikov, A.O. Infrastruktura kak kod: formiruetsya novaya real'nost' informacionnoj bezopasnosti / A.O. Kalashnikov, K.A. Bugajskij // Informaciya i bezopasnost'. – 2019. – T. 22, № 4. – pp. 495-506.
13. Bugajskij, K.A. Rasshirennaya model' otkrytyh sistem (CHast' 1) / K. A. Bugajskij, D. S. Birin, B. O. Deryabin, S. O. Cependa // Informaciya i bezopasnost'. – 2022. – T. 25, № 2. – pp. 169-178. – DOI 10.36622/VSTU.2022.25.2.001.
14. Kalashnikov A.O. Primenenie logiko-veroiatnostnogo metoda v informatsionnoi bezopasnosti (Chast 1) / Kalashnikov A.O., Bugaiskii K.A., Birin D.S., Deriabin B.O., Tsependa S.O., Tabakov K.V. // Voprosy kiberbezopasnosti. – 2023. – №4(56) – pp. 23-32.
15. Kalashnikov A.O. Primenenie logiko-veroiatnostnogo metoda v informatsionnoi bezopasnosti (Chast 2) / Kalashnikov A.O., Bugaiskii K.A., Anikina E. I., Pereskokov I.S., Petrov An.O., Petrov Al.O., Khramchenkova E.S., Molotov A.A. // Voprosy kiberbezopasnosti. – 2023. – №5(57). – pp. 113-127. DOI:10.21681/2311-3456-2023-6-113-127.
16. Bugajskij, K.A. Rasshirennaya model' otkrytyh sistem (CHast' 2) / K.A. Bugajskij, I.S. Pereskokov, A.O. Petrov, A.O. Petrov // Informaciya i bezopasnost'. – 2022. – T. 25, № 3. – pp. 321-330. – DOI 10.36622/VSTU.2022.25.3.001.
17. Bugajskij, K.A. Rasshirennaya model' otkrytyh sistem (CHast' 3) / K.A. Bugajskij, B.O. Deryabin, K.V. Tabakov, E.S. Hramchenkova, S.O. Cependa // Informaciya i bezopasnost'. – 2022. – T. 25, № 4. – pp. 501-512.
18. Kalashnikov, A. O. Model kolichestvennogo otsenivaniia agenta slozhnoi seti v usloviiakh nepolnoi informirovannosti / A. O. Kalashnikov, K. A. Bugaiskii // Voprosy kiberbezopasnosti. – 2021. – № 6(46). – pp. 26-35. – DOI 10.21681/2311-3456-2021-6-26-35.
19. Kotenko I. V. Tekhnologii bolshikh dannykh dlia korreliatsii sobytii bezopasnosti na osnove ucheta tipov sviazei / I. V. Kotenko, A. V. Fedorchenko, I. B. Saenko, A. G. Kushnerevich // Voprosy kiberbezopasnosti. – 2017. – № 5(24). – pp. 2-16. – DOI 10.21681/2311-3456-2017-5-2-16.
20. Doinikova, E. V. Sovershenstvovanie grafov atak dlia monitoringa kiberbezopasnosti: operirovanie netochnostiami, obrabotka tsiklov, otobrazhenie intsidentov i avtomaticheskii vybor zashchitnykh mer / E. V. Doinikova, I. V. Kotenko // Trudy SPIIRAN. – 2018. – № 2(57). – pp. 211-240.
21. Kulik, B. A. Logika i matematika: prosto o slozhnykh metodakh logicheskogo analiza / B. A. Kulik. – Sankt-Peterburg: Izdatelstvo «Politekhnika», 2021. – 141 p. – ISBN 978-5-7325-1166-6. – DOI 10.25960/7325-1166-6.