УДК 004.056

В.В. Баранов, А.А. Шелупанов

Методика и алгоритмы расчета защищенности элементов распределенных информационных систем в условиях деструктивного воздействия

Проведено обоснование актуальности разработки методического аппарата и алгоритмов определения объектов деструктивного воздействия и расчета параметров защищенности распределенных информационных систем. Осуществлен анализ исследований в данной области, сформулированы требования к функциональным возможностям методики. Выбран математический аппарат, разработаны методика и алгоритмы определения объектов деструктивного воздействия на различных уровнях интегрированных онтологических структурно-функциональных нейро-байесовских моделей, а также степени их критичности для функциональной и структурной живучести типовых информационных модулей распределённых информационных систем. Дан порядок расчета параметров защищенности типовых информационных модулей и оценки эффективности защитных мер.
Ключевые слова: онтологическая модель, нейро-байесовская модель, объекты воздействия, уязвимости, структурная живучесть, функциональная живучесть, меры защиты информации.
DOI: 10.21293/1818-0442-2022-25-4-88-100

Обеспечение надежной защиты распределенных информационных систем (РИС) требует разработки методического аппарата моделирования процессов их функционирования в условиях деструктивного воздействия (ДВ) различных категорий нарушителей и расчета параметров их защищенности. На практике данная задача осложняется вероятностной оценкой, неполными данными и большой степенью неопределенности в характере действий нарушителя, выборе им тех или иных способов реализации угроз безопасности информации (УБИ).

Научная ценность данного исследования заключается в том, что представленные методика и алгоритмы позволяют определять объекты ДВ на различных уровнях типовых информационных модулей распределенных информационных систем (ТИМ РИС), осуществлять расчет степени их критичности для функциональной и структурной живучести системы. Разработан новый способ моделирования ТИМ РИС, заключающийся в интеграции онтологических структурно-функциональных и нейро-байесовских моделей (ОСФ-НБМ). Такой подход вносит определенный вклад в развитие теории и методологии информационной безопасности (ИБ) и является логическим продолжением проведенных ранее авторами исследований.

В работе принят ряд ограничений. Так, не рассматриваются алгоритмы разработки интегрированных ОСФ-НБМ ТИМ РИС. Концептуально представлен облик нейро-байесовских моделей (НБМ). Данные области можно определить как направления дальнейших исследований.

Ключевым аспектом в процессе решения рассматриваемой в работе проблемы является обеспечение требуемого уровня результатов моделирования событий ИБ, связанных с оценкой численных значений показателей способов реализации УБИ и применения организационных и технических мер защиты информации (МЗИ). На этапе функционирования в условиях динамично меняющегося ДВ система защиты РИС требует непрерывного мониторинга и адекватного реагирования на новые риски реализации УБИ. Данное обстоятельство определяет потребность моделирования динамики изменения событий ИБ и отражения их показателей. В этих целях применяется математический аппарат многокритериальной оценки (методов MCDM). Из множества альтернативных вариантов решений по нескольким критериям выбирается наиболее эффективный для складывающейся обстановки вариант. Обзор таких методов приведен в [1, 2].

В работе [3] предложен оригинальный гибридный многокритериальный метод оценки AHP-TOPSIS-2N, представляющий собой интеграцию процесса аналитической иерархии (Analytic Hierarchy Process, AHP), метода предпочтения порядка по сходству с идеальным решением (Technique for Order Preference by Similarity to Ideal Solution, TOPSIS) и двух процедур нормализации (2N).

Подход к решению задачи моделирования процесса оценки защищенности РИС, которая послужила основой для создания системы поддержки принятия решений (СППР) должностных лиц органов управления (ДЛ ОУ) в области ИБ, представлен в [4]. Он заключается в интеграции онтологических структурно-функциональных и нейро-байесовских моделей для составления ациклического графа, отражающего вероятностные показатели структурно-функциональных связей событий ИБ различного генеза.

Для решения проблемы разработки представленной в работе методики был проанализирован ряд научных исследований и регулятивных документов в данной области.

В [5, 6] представлены основные понятия и критерии оценки защищенности РИС. Защита от УБИ осуществляется применением МЗИ. МЗИ подразделяются на технические меры (ТМ), реализуемые

средствами защиты информации (СЗИ), и организационные меры (ОМ), реализуемые режимными мероприятиями. Совокупность применяемых ОМ и ТМ представляет собой способ защиты информации. При этом вклад указанных видов МЗИ в процесс защиты не всегда симметричен.

В [7] определено, что объекты воздействия должны быть установлены на аппаратном, программном, прикладном, сетевом и пользовательском уровнях. Приведены примеры сценариев, тактик и техник атак. Предложен экспертный метод оценки актуальности УБИ.

В исследовании [8] предлагается с помощью адаптивного мониторинга определять объекты ДВ, наиболее подверженные атакам, и акцентировать внимание на их защите.

В научной работе [9] представлена методика риск-ориентированного моделирования атак, основанная на ранжировании рисков получения ущерба и позволяющая выявить наиболее «опасные» с этой точки зрения объекты.

Процесс передачи и хранения данных отображает открытая сетевая модель «Basic Reference Model Open Systems Interconnection model», или сокращенно OSI/ISO, которая имеет семь уровней [10]. С ее помощью легко определить структурно-функциональные связи элементов локальных информационно-вычислительных сетей (ЛИВС) и РИС в целом. Данная модель также описывает все, что происходит при отправке и приеме данных, а также участвующие в этом процессе физические и логические устройства, интерфейсы и протоколы.

Современные подходы, связанные с разработкой СППР и применением искусственного интеллекта для решения задач управления, представлены в [11, 12].

Объекты воздействия на разных уровнях реализуют процессы различной степени критичности для обеспечения устойчивого функционирования РИС и ее элементов. В настоящее время их взаимное влияние и показатели безопасности на интегративном уровне слабо исследованы [13].

Проведенный ранее анализ показал, что существующие методические подходы не содержат апробированный математический аппарат расчета зависимости показателей защищенности РИС от тех или иных способов реализации УБИ. Поэтому принимаемые решения в большей степени носят субъективный характер, достоверность которых зависит от качества имеющихся исходных данных по складывающейся обстановке, а также практического опыта экспертов.

Данное обстоятельство определяет **научную задачу исследования**, которая заключается в разработке новых и совершенствовании существующих методических и инструментальных средств расчета численных значений показателей событий ИБ различного генеза.

Научную задачу, поставленную в исследовании, целесообразно декомпозировать на две подзадачи. Первая будет касаться процесса моделирования объектов ДВ в ТИМ РИС, а вторая – методов и алгоритмов расчета параметров их защищенности.

В ходе анализа существующих методов моделирования были выбраны следующие наиболее подходящие для моделирования объектов ДВ в ТМ РИС. Это метод онтологий для формирования онтологических структурно-функциональных моделей (ОСФМ) [14, 15] и метод байесовских сетей для формирования нейро-байесовской модели (НБМ) [16, 17].

Онтологии служат для систем организации знаний и применяются в тех областях, где требуется обнаружить инфраструктурную интеграцию, выявить скрытые взаимосвязи между элементами. Основной постулат онтологии: если в базе знаний отсутствуют некоторые объекты или связи между ними, то это не значит, что они не существуют, а просто они не описаны.

Онтология может быть представлена в виде графа, вершины которого – это сущности (концепты), а ребра – отношения между сущностями. Если любое утверждение можно представить в виде простых предложений, то из них можно извлечь данные по упомянутым в них сущностям (концептам) и отношениям между ними. В зависимости от целей и задач может быть построено онтологическое пространство знаний, включающее в себя модули подсистем с отражением реализуемых ими процессов [18].

В области ИБ и применительно к данному исследованию это свойство онтологий может быть реализовано для построения онтологического пространства знаний, включающего онтологии ТИМ РИС с требуемой степенью детализации, онтологии объектов ДВ в ТИМ РИС и их уязвимостей, онтологии рисков УБИ, способов и сценариев их реализации, а также онтологии защитных мероприятий [19].

Важным преимуществом онтологий является их наглядность. Это дает возможность построения ОСФМ объектов ДВ в ТИМ РИС любой сложности, а также определение путей (маршрутов) реализации сценария УБИ внутри системы, идентификацию, анализ и оценивание рисков инцидентов, а также способы и точки нейтрализации УБИ и (или) уязвимостей.

Для полноценной работы модели необходима вероятностная оценка наступления взаимоувязанных событий ИБ. Например, вероятность риска инцидента при реализации с определенной вероятностью сценария УБИ. Такая вероятность называется условной, т.е. она для одного события наступает при условии, что другое событие (по подтверждённому или неподтверждённому доказательством утверждению) уже произошло. Для вычисления таких вероятностей применяется теорема Байеса, суть которой описывает следующая формула:

$$P(A|B)\,P(B) = P(B|A)\,P(A), \qquad (1)$$

где P – условная вероятность событий A и B.

Графическая модель данной зависимости представляет собой байесовскую сеть доверия – направ-

ленный ациклический граф, т.е. граф, в котором не существует направленного маршрута, начинающегося и заканчивающегося в одной и той же вершине [20].

Вершины сети представляет собой множество случайных величин, определяющих состояние событий ИБ и подчиняющихся закону Гаусовского распределения. Вершины могут описываться с помощью набора переменных, для которых задаются взвешенные параметры и формируется множество гипотез.

В исследовании вершинами графа байесовской модели приняты концепты онтологической модели ДВ в ТИМ РИС. Это позволило определить значения условных вероятностей функциональных связей концептов, которые являются ребрами графа. Таким образом, можно заключить, что в ходе исследования выявлено свойство интегративности ОСФМ и НБМ, которое и будет применено для моделирования объектов ДВ в ТИМ РИС.

Для решения второй подзадачи научного исследования применены методы алгебраических матриц, элементы теории графов, методы многокритериальной оценки (MCDM), методы теории нейро-сетевого анализа.

В ряде работ [21, 22] события ИБ деструктивного характера формализованно представлены в виде векторов атак, отражающих показатели их существенных свойств и точки (объекты) воздействия.

Для представления множества показателей защищенности объектов ДВ разных уровней ТИМ РИС применен метод алгебраических матриц, позволяющий формализовать и структурировать их в соответствии с целями исследования [23].

В научной работе [24] была предложена новая гибридная методика PROMETHEE-SAPEVO-M1, основанная на многокритериальных методах оценки. Она реализована на основе интеграции двух методов – PROMETHEE [25] и SAPEVO-M [26]. Предложенный методический подход позволяет проводить детальную количественную и качественную оценку массивов исходных данных, структурировать формат для расчета весовых коэффициентов предпочтительности показателей, критериев и альтернатив.

Наиболее ценной ее стороной является возможность оптимизации количества критериев с помощью их классификации на базе факторного анализа.

Данные модели и методики имеют программную реализацию [27], разработанную на языке Python, что обеспечивает информационно-аналитическую поддержку принимающему решения должностному лицу в процессе анализа и оценки объекта относительно требуемых критериев.

Применение указанных методов позволит провести первичный расчет весов событий ИБ для ввода их в НБМ.

Для обучения рассматриваемой в работе НБМ может быть применен предложенный в исследовании [28] вариант алгоритма обучения искусственного интеллекта семейства AutoAI. Данный алгоритм существенно снижает существующие недостатки самообучающихся систем искусственного интеллекта и обладает следующими преимуществами:

– реализует количественный «причинно-сравнительный анализ» на основе синтезированных обучающих данных о событиях ИБ, которые уже произошли;

– реализует количественное «корреляционное исследование», где оценивается статистическая взаимосвязь между уже свершившимися и еще не свершившимися событиями ИБ и определяются их взаимное влияние и фактические риски;

– алгоритм AutoAI может прогнозировать фактические потери, включая свершившиеся и возможные риски потерь от деструктивных событий ИБ;

– в конструкциях сценариев обучения используется стандартная аналитика с открытым исходным кодом (OSINT) для сбора общедоступных данных, включая общедоступные хранилища (базы данных);

– рассматриваемый алгоритм AutoAI и метод FAIR (метод справедливого распределения ресурсов из теории игр) интегрированы с использованием байесовской оптимизации в качестве вероятностного итеративного алгоритма, основанного на гауссовском процессе или графовой модели и функции сбора обучающих данных по направлениям «разведка» и «функционирование».

Таким образом, рассматриваемый алгоритм обучения искусственного интеллекта по своим структурным и функциональным характеристикам может быть адаптирован для обеспечения безопасности РИС.

Далее исследуем практическое применение выбранных методов моделирования для определения структурно-функциональных связей событий ИБ в РИС и их вероятностных значений.

Результаты и обсуждение

Структурно РИС можно представить совокупностью определенного количества ТИМ различного назначения. В работе определены следующие их виды. Первый из них представляют локальные информационно-вычислительные сети (ЛИВС). ТИМ второго вида – центры обработки данных (ЦОД), а третьего вида – удаленные пользователи (УП). Структура РИС определяется количеством видов ТИМ, количеством и составом элементов, что обеспечивает достижение свойства универсальности и масштабируемости моделирования.

Для определения в составе ТИМ РИС потенциальных объектов ДВ, были выделены концепты восьми уровней, соответствующих уровням модели MBOC/ISO: физического, канального, сетевого, транспортного, сеансового, представительского и прикладного, а также дополнительно включенного пользовательского уровня. Такой подход позволил идентифицировать функциональные процессы между концептами ТИМ РИС на различных уровнях. На рис. 1 представлена структура функциональных связей ТИМ РИС вида ЛИВС на сетевом и аппаратном уровнях.

В ходе построения онтологии ЛИВС можно определить функциональные связи между концептами различных уровней, а также через какие физические и логические интерфейсы на какие объекты может быть осуществлено ДВ, т.е. определить маршруты реализации сценариев УБИ.

Это позволило разработать ОСФМ объектов ДВ на каждом из уровней ТИМ РИС. В качестве примера (рис. 2) приведен фрагмент ОСФМ объектов ДВ на представительском уровне ТИМ РИС. Их уязвимости можно определить из соответствующих баз данных (БДУ).

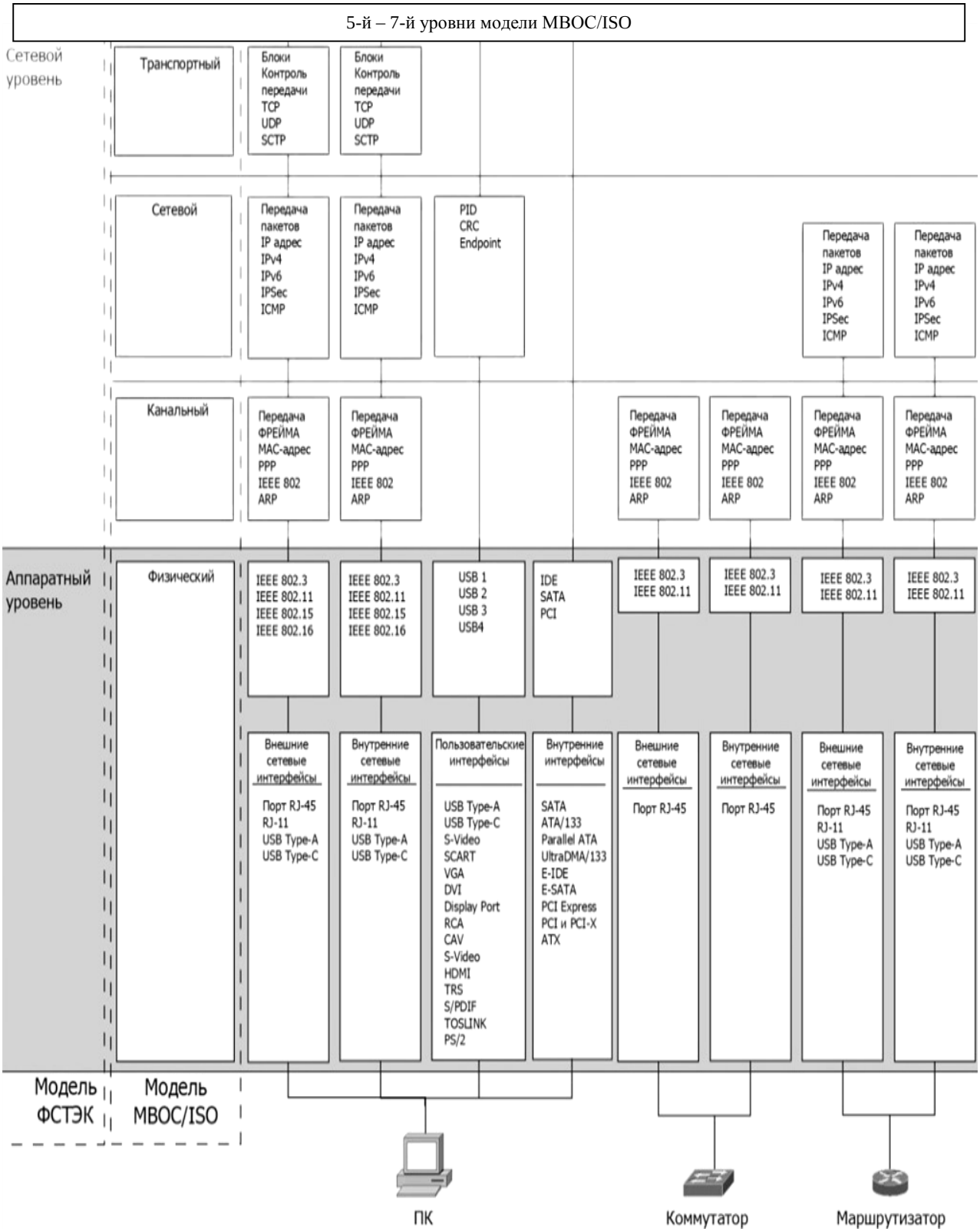

Рис. 1. Концепты и их функциональные связи на сетевом и аппаратном уровнях модели MBOC/ISO для ТИМ вида ЛИВС

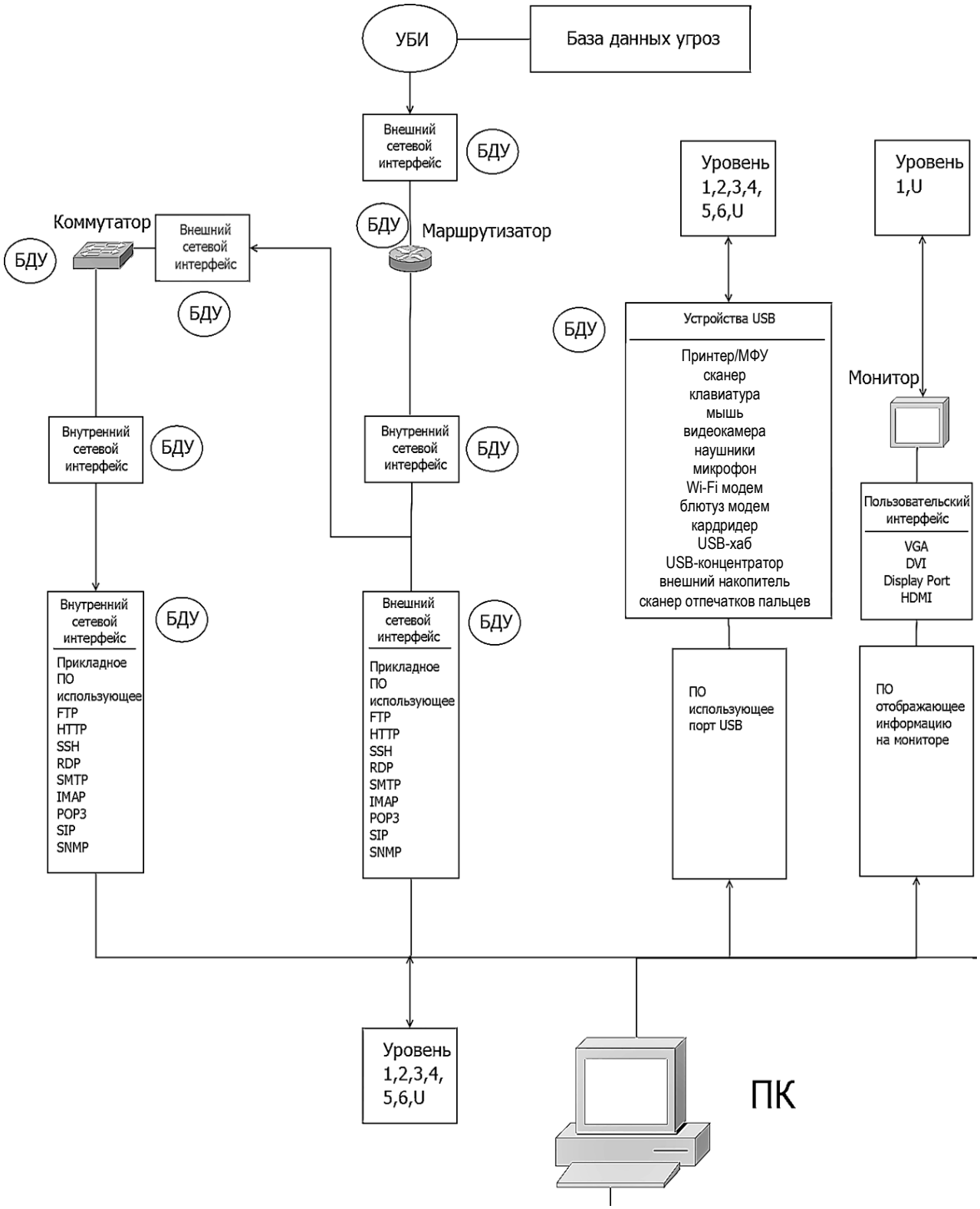

Рис. 2. Онтологическая структурно-функциональная модель объектов ДВ на представительском уровне ТИМ РИС (фрагмент)

Данные модели взаимно интегрированы и предназначены для проведения ситуационного анализа и выявления параметров, определяющих характеристики вектора ДВ на объекты восьми уровней ТИМ РИС, точки и маршруты воздействия применяемых защитных мер, взаимосвязи событий ИБ и степени их взаимовлияния. В таблице концептуально сведены объекты ДВ на уровнях модели.

Онтологические модели алгоритмично связаны с нейро-байесовскими. Основу НБМ составляют типовые кластеры, отражающие вероятностные характеристики процесса функционирования защищаемой РИС в условиях ДВ (рис. 3).

Объекты ДВ на уровнях модели

Уровни модели	Объекты деструктивного воздействия
Пользовательский	Данные пользователя (идентификационные, аутентификационные, персональные, корпоративные), информационные ресурсы
Прикладной	Прикладное программное обеспечение (ПО) (офисное, систем электронного документооборота, браузеров, моделирования, расчетное и др.)
Представительский	Операционные системы, системное ПО, системные библиотеки, платформы виртуализации. ПО поддержки протоколов
Сеансовый	Операционные системы, системное ПО, системные библиотеки, платформы виртуализации. ПО поддержки протоколов
Транспортный	Операционные системы, системное ПО, системные библиотеки, платформы виртуализации. ПО поддержки протоколов
Сетевой	Передаваемые данные (информационные, служебные и технические). Пакеты сообщений
Канальный	Передаваемые данные (информационные, служебные и технические)
Физический	Аппаратное обеспечение ПК, серверов, систем хранения данных, коммутационного и маршрутизирующего оборудования, периферийных и сетевых устройств, элементов ТКС. Каналы связи и среда передачи данных

Каждый типовой кластер НБМ представлен направленным ациклическим графом. Узлы данного графа являются событиями ИБ, выраженными отдельными вероятностными величинами, а его ребра являются условными зависимостями, подчиняющимися Гаусовскому распределению условных вероятностей.

Применив свойство симметричности байесовских и онтологических моделей, примем, что узлы байесовской сети будут соответствовать концептам онтологических моделей, а ребра – их функциональным связям. Данное свойство позволит НБМ выполнить задачу по расчету условных вероятностей событий ИБ, структурно отраженных ОСФМ. Рассмотрим более подробно данный процесс.

Каждый типовой кластер НБМ отражает события ИБ, связанные с риском реализации одной УБИ, посредством эксплуатации множества уязвимостей объекта воздействия (концепта ОСФМ) каким-либо способом и ее локализацией посредством применения ОМ и ТМ. Рассматриваются два исхода: УБИ локализована и УБИ реализована и привела к инциденту ИБ.

В составе типового кластера НБМ выделены четыре зоны событий ИБ.

1. Зона формирования рисков УБИ.
2. Зона ликвидации рисков УБИ.
3. Зона формирования рисков инцидента.
4. Зона ликвидации последствий инцидента.

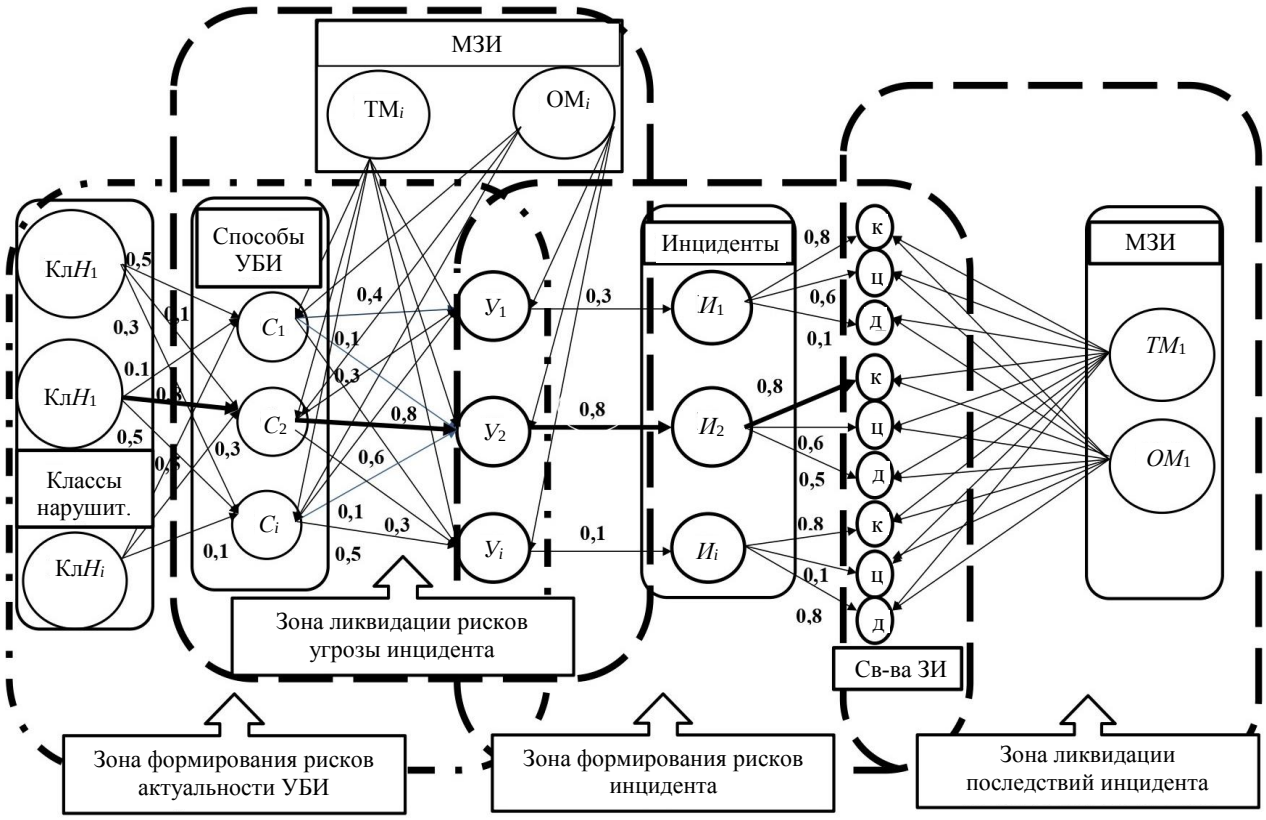

Рис. 3. Типовой кластер НБМ построения защиты элемента РИС

На сформированные ОСФМ симметрично накладывается структура типовых кластеров НБМ. Исходные данные для НБМ получаем из разработанных ОСФМ по направлению событий ИБ деструктивного и защитного характера. Весовые коэффициенты событий ИБ рассчитываются с помощью применения программного продукта PROMETHEE-SAPEVO-M1.

Зона рисков УБИ формируется на основе ОСФМ ТИМ РИС, взаимосвязей сценариев их реализации и уязвимостей объектов воздействия.

Численные значения вероятности выбора нарушителем способа реализации УБИ $P(C_i)$ будут зависеть от его возможностей, затрачиваемых ресурсов, ценности защищаемых активов, структуры ТИМ РИС, применяемых МЗИ, а также актуальных уязвимостей [29].

Применение алгоритма обучения НБМ AutoAI позволяет произвести расчет вероятностных характеристик актуальности УБИ, способов и сценариев их реализации с учетом взаимного влияния свершившихся и прогнозируемых событий ИБ, а также выбрать необходимые для их локализации ОМ и ТМ. Фрагмент данного процесса отражен на рис. 4.

Оценка защищенности ТИМ РИС осуществляется в соответствии с регулятивными документами. Эффективность способов защиты имеет вероятностные характеристики, зависящие от вектора показателей защитных мероприятий и вектора показателей способов и сценариев ДВ, а также выявленных новых актуальных уязвимостей.

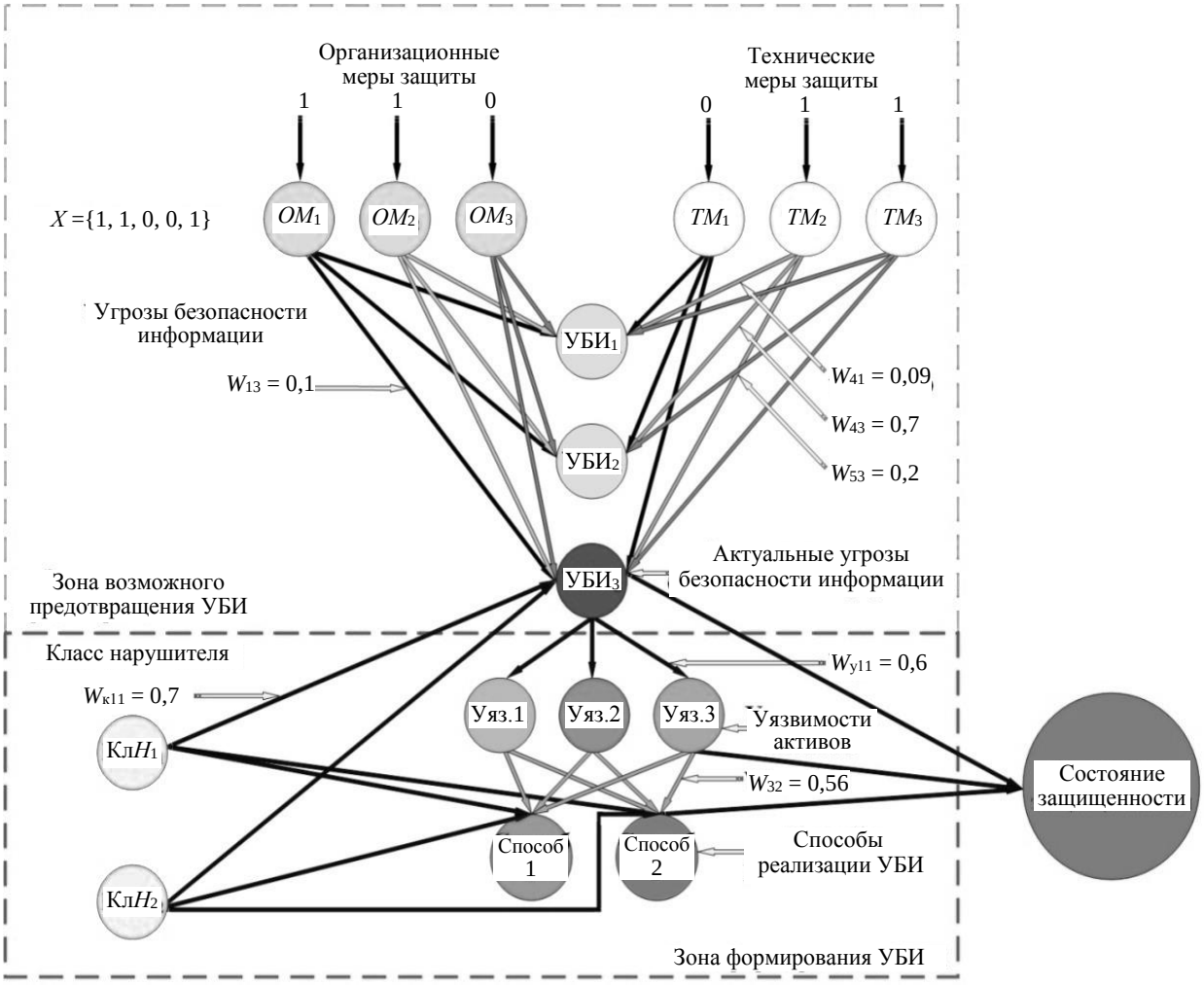

Рис. 4. Работа НБМ по определению вероятностных характеристик защищенности

Рассмотрим содержание методики и алгоритмов для расчета численных показателей оценки защищенности объектов ДВ.

Представленная в работе методика позволяет осуществлять универсальную оценку событий ИБ различного генеза по численным значениям показателей защитных и деструктивных воздействий. Такой подход минимизирует вероятность принятия неэффективного решения.

Рассмотрим алгоритм ее применения для ранее разработанной ОСФ-НБМ.

Каждая РИС состоит из ТИМ различного типа и структуры. Обозначим их через множество $\{G_1 \ldots G_i\}$. В каждом ТИМ выделены восемь уровней его структуры для определения объектов деструктивного воздействия. То есть

$$G_i \in \{F_i, K_i, L_i, T_i, S_i, A_i, P_i, H_i\}, \quad (2)$$

где F_i – физический, K_i – канальный, L_i – сетевой, T_i – транспортный, S_i – сеансовый, A_i – представительский, P_i – прикладной, H_i – пользовательский уровни i-го ТИМ.

В модели потенциальные объекты ДВ на данных уровнях представлены концептами, соединенными между собой функциональными связями.

$$K_i \in \left\{ \sum_1^m K_{F_i}, \sum_1^m K_{k_i}, \sum_1^m K_{L_i}, \sum_1^m K_{T_i}, \sum_1^m K_{S_i}, \sum_1^m K_{A_i}, \sum_1^m K_{P_i}, \sum_1^m K_{H_i} \right\}. \quad (3)$$

Каждый из данных концептов имеет определенный набор уязвимостей $\{Y_1 \ldots Y_n\}$. Уязвимости определяются в ходе проведения пентестинга и (или) мероприятий мониторинга и аудита ИБ. Обозначим эти мероприятия через индекс T_i, где i – вид тестирования на каждом из уровней. Для каждого информационного модуля введем понятие кортежа его уязвимостей, выявленных в ходе тестирования на каждом из уровней:

$$\mathbf{y}_{T_i} \in \left\{ \sum_1^n Y_{F_i}, \sum_1^n Y_{k_i}, \sum_1^n Y_{L_i}, \sum_1^n Y_{T_i}, \sum_1^n Y_{S_i}, \sum_1^n Y_{A_i}, \sum_1^n Y_{P_i}, \sum_1^n Y_{H_i} \right\}. \quad (4)$$

Для обеспечения привязки данного вектора к онтологической модели составим следующие матрицы уязвимостей концептов каждого уровня. В столбцах матрицы отображаются концепты соответствующего уровня, а в строках – обнаруженные уязвимости каждого из концептов:

$$\mathbf{G}_{iF_i} = \begin{bmatrix} K_{1F_i}Y_1 & K_{1F_i}Y_2 & \ldots & K_{1F_i}Y_n \\ K_{2F_i}Y_1 & K_{2F_i}Y_2 & \ldots & K_{2F_i}Y_n \\ K_{3F_i}Y_1 & K_{3F_i}Y_2 & \ldots & K_{3F_i}Y_n \\ K_{mF_i}Y_1 & K_{mF_i}Y_2 & \ldots & K_{mF_i}Y_n \end{bmatrix}, \quad (5а)$$

$$\mathbf{G}_{iK_i} = \begin{bmatrix} K_{1K_i}Y_1 & K_{1K_i}Y_2 & \ldots & K_{1K_i}Y_n \\ K_{2K_i}Y_1 & K_{2K_i}Y_2 & \ldots & K_{2K_i}Y_n \\ K_{3K_i}Y_1 & K_{3K_i}Y_2 & \ldots & K_{3K_i}Y_n \\ K_{mK_i}Y_1 & K_{mK_i}Y_2 & \ldots & K_{mK_i}Y_n \end{bmatrix}, \quad (5б)$$

$$\mathbf{G}_{iL_i} = \begin{bmatrix} K_{1L_i}Y_1 & K_{1L_i}Y_2 & \ldots & K_{1L_i}Y_n \\ K_{2L_i}Y_1 & K_{2L_i}Y_2 & \ldots & K_{2L_i}Y_n \\ K_{3L_i}Y_1 & K_{3L_i}Y_2 & \ldots & K_{3L_i}Y_n \\ K_{mL_i}Y_1 & K_{mL_i}Y_2 & \ldots & K_{mL_i}Y_n \end{bmatrix}, \quad (5в)$$

$$\mathbf{G}_{iT_i} = \begin{bmatrix} K_{1T_i}Y_1 & K_{1T_i}Y_2 & \ldots & K_{1T_i}Y_n \\ K_{2T_i}Y_1 & K_{2T_i}Y_2 & \ldots & K_{2T_i}Y_n \\ K_{3T_i}Y_1 & K_{3T_i}Y_2 & \ldots & K_{3T_i}Y_n \\ K_{mT_i}Y_1 & K_{mT_i}Y_2 & \ldots & K_{mT_i}Y_n \end{bmatrix}, \quad (5г)$$

$$\mathbf{G}_{iS_i} = \begin{bmatrix} K_{1S_i}Y_1 & K_{1S_i}Y_2 & \ldots & K_{1S_i}Y_n \\ K_{2S_i}Y_1 & K_{2S_i}Y_2 & \ldots & K_{2S_i}Y_n \\ K_{3S_i}Y_1 & K_{3S_i}Y_2 & \ldots & K_{3S_i}Y_n \\ K_{mS_i}Y_1 & K_{mS_i}Y_2 & \ldots & K_{mS_i}Y_n \end{bmatrix}, \quad (5д)$$

$$\mathbf{G}_{iA_i} = \begin{bmatrix} K_{1A_i}Y_1 & K_{1A_i}Y_2 & \ldots & K_{1A_i}Y_n \\ K_{2A_i}Y_1 & K_{2A_i}Y_2 & \ldots & K_{2A_i}Y_n \\ K_{3A_i}Y_1 & K_{3A_i}Y_2 & \ldots & K_{3A_i}Y_n \\ K_{mA_i}Y_1 & K_{mA_i}Y_2 & \ldots & K_{mA_i}Y_n \end{bmatrix}, \quad (5е)$$

$$\mathbf{G}_{iP_i} = \begin{bmatrix} K_{1P_i}Y_1 & K_{1P_i}Y_2 & \ldots & K_{1P_i}Y_n \\ K_{2P_i}Y_1 & K_{2P_i}Y_2 & \ldots & K_{2P_i}Y_n \\ K_{3P_i}Y_1 & K_{3P_i}Y_2 & \ldots & K_{3P_i}Y_n \\ K_{mP_i}Y_1 & K_{mP_i}Y_2 & \ldots & K_{mP_i}Y_n \end{bmatrix}, \quad (5ж)$$

$$\mathbf{G}_{iH_i} = \begin{bmatrix} K_{1H_i}Y_1 & K_{1H_i}Y_2 & \ldots & K_{1H_i}Y_n \\ K_{2H_i}Y_1 & K_{2H_i}Y_2 & \ldots & K_{2H_i}Y_n \\ K_{3H_i}Y_1 & K_{3H_i}Y_2 & \ldots & K_{3H_i}Y_n \\ K_{mH_i}Y_1 & K_{mH_i}Y_2 & \ldots & K_{mH}Y_n \end{bmatrix} \quad (5з)$$

где матрицы – уязвимости концептов соответствующих уровней: (5а) – физического; (5б) – канального; (5в) – сетевого; (5г) – транспортного; (5д) – сеансового; (5е) – представительского; (5ж) – прикладного; (5з) – пользовательского. Таким образом, мы получаем множество распределенных по уровням модели ТИМ РИС объектов ДВ и их уязвимостей, которые будут являться точками доступа для реализации УБИ каким-либо способом.

Далее предлагается провести ранжирование концептов путем присвоения им весов влияния на живучесть ТИМ РИС. В частности, вводим матрицу векторов критической значимости концептов каждого уровня ТИМ РИС следующего вида:

$$\mathbf{W}_{\mathbf{G}_i} = \begin{bmatrix} \mathbf{w}_{1K_{F_i}} & \mathbf{w}_{2K_{F_i}} & \mathbf{w}_{3K_{F_i}} & \ldots & \mathbf{w}_{mK_{F_i}} \\ \mathbf{w}_{1K_{K_i}} & \mathbf{w}_{2K_{K_i}} & \mathbf{w}_{3K_{K_i}} & \ldots & \mathbf{w}_{mK_{K_i}} \\ \mathbf{w}_{1K_{L_i}} & \mathbf{w}_{2K_{L_i}} & \mathbf{w}_{3K_{L_i}} & \ldots & \mathbf{w}_{mK_{L_i}} \\ \mathbf{w}_{1K_{T_i}} & \mathbf{w}_{2K_{T_i}} & \mathbf{w}_{3K_{T_i}} & \ldots & \mathbf{w}_{mK_{T_i}} \\ \mathbf{w}_{1K_{S_i}} & \mathbf{w}_{2K_{S_i}} & \mathbf{w}_{3K_{S_i}} & \ldots & \mathbf{w}_{mK_{S_i}} \\ \mathbf{w}_{1K_{A_i}} & \mathbf{w}_{2K_{A_i}} & \mathbf{w}_{3K_{A_i}} & \ldots & \mathbf{w}_{mK_{A_i}} \\ \mathbf{w}_{1K_{P_i}} & \mathbf{w}_{2K_{P_i}} & \mathbf{w}_{3K_{P_i}} & \ldots & \mathbf{w}_{mK_{P_i}} \\ \mathbf{w}_{1K_{H_i}} & \mathbf{w}_{2K_{H_i}} & \mathbf{w}_{3K_{H_i}} & \ldots & \mathbf{w}_{mK_{H_i}} \end{bmatrix}. \quad (6)$$

Вес (значимость) i-го концепта определяется для живучести ТИМ РИС в целом. Весовые коэффициенты определяются экспертным методом из анализа ОСФМ.

Значения весов могут изменяться в пределах от 0 до 1. Критическую значимость весов определим в интервале от 0,8 до 1.

Введем правило: «Если уязвимость в ходе тестирования вскрыта, то она должна быть защищена применением технических средств или организационных мероприятий». Для этого мы формируем матрицу векторов защитных мероприятий.

В этих целях необходимо проделать следующее.

1. Актуализировать угрозы УБИ и сценарии их реализации с применением кластера НБМ.

2. Актуализировать перечень доступных для ДВ концептов и их уязвимостей (5а)–(5з). Данные связи прописаны в базах данных.

3. Составить матрицу распределения СЗИ и проводимых режимных мероприятий. Данные связи прописаны в базах данных и базах знаний.

4. Подключить кластер НБМ, ввести данные по проведенным защитным мероприятиям.

5. Вывести отчет и убедиться, что все уязвимости закрыты и (или) риски реализации сценариев УБИ локализованы.

Однако опыт подсказывает, что абсолютно защищенных РИС нет. Это объясняется следующими причинами:

- не все уязвимости вскрыты в ходе тестирования;
- компьютерная разведка противника применила новый способ вскрытия объектов воздействия;
- противник разработал новый сценарий атаки, позволяющий обойти применяемые СЗИ;
- противник уничтожил (заблокировал) применяемые СЗИ;
- СЗИ вышли из строя в ходе эксплуатации или параметры их были настроены неправильно;
- противник получил физический доступ к элементам ИС и (или) к системе защиты информации.

В данном ракурсе весьма актуальной будет методика определения потенциальной возможности ДВ на концепты ТИМ РИС.

Для определения потенциальной возможности ДВ на концепты необходимо провести следующие действия:

1. Для каждого ТИМ РИС введем понятие вектора вероятностей обнаружения его уязвимостей компьютерной разведкой противника (7):

$$\mathbf{G}_{P_i} \in \{P_{У_1}, P_{У_2}, \ldots, P_{У_n}\}. \quad (7)$$

2. Составим матрицы вероятностей вскрытия уязвимостей ($\mathbf{P}_{\text{вск.}У_i}$), вскрытия элементов системы защиты ($\mathbf{P}_{\text{вск.СЗ}_i}$).

3. Составим матрицы вероятностей выживания i-го информационного модуля ($\mathbf{P}_{\text{выж.ТИМ}_i}$) при физическом, программном воздействии и при эксплуатации уязвимостей концептов.

4. Составим матрицы вероятностей выживания элементов системы защиты ($\mathbf{P}_{\text{выж.СЗ}_i}$) при физическом и (или) программном воздействии.

5. Составим матрицы вероятностей сохранения работоспособности при воздействии преднамеренных или непреднамеренных радиоэлектронных помех на средства защиты ($\mathbf{P}_{\text{сп.СЗ}_i}$) и элементы ТИМ ($\mathbf{P}_{\text{сп.ЭТИМ}_i}$).

6. Составим матрицы вероятностей исправного функционирования средств защиты ($\mathbf{P}_{\text{над.СЗИ}_i}$) и элементов ТИМ ($\mathbf{P}_{\text{над.ЭТМИ}_i}$) в ходе эксплуатации в условиях критического изменения параметров, в том числе и при ошибочных действиях персонала.

Расчет вероятностных характеристик пп. 3–6 должен производиться с учетом весов критичности концептов ТИМ на всех его уровнях [30].

Отмеченное ранее в исследовании свойство интегративности байесовских и онтологических моделей позволило разработать методику расчета указанных выше вероятностных характеристик деструктивного воздействия с помощью НБМ.

Порядок расчета изменения численных значений показателей защищенности ТИМ РИС в ходе функционирования представлен в следующей методике.

Суть его заключается в возможности получать обновленные значения вероятностных характеристик новых событий ИБ по мере получения информации о них.

В математической модели Байеса узлы графа, являющиеся событиями ИБ типа «Объект ДВ – уязвимость», будут получать информацию от кластеров ДВ и кластеров защитных мероприятий по мере ее поступления. При этом возможен одновременный ввод информации о событиях ИБ различного генеза в несколько узлов.

В ТИМ РИС взаимное влияние ДВ и защитных мер представлено в виде различных по структуре цепочек событий: последовательных, сходимых и расходимых.

При этом в цепочках последовательных событий могут быть однородные – (рис. 5 *а*, *б*) и разнородные – (деструктивные и защитные) события ИБ (рис. 5, *в*–*е*).

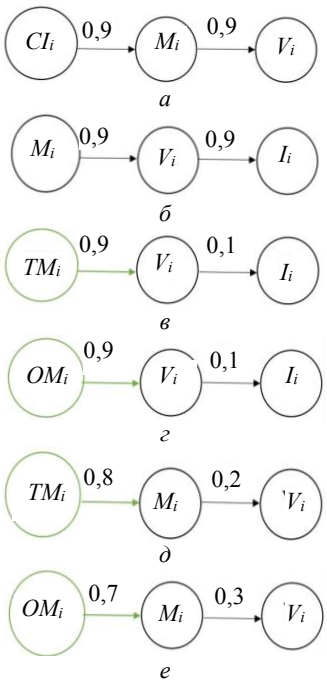

Рис. 5. Виды цепочек последовательных событий:
а, *б* – цепочки однородных (деструктивных) событий;
в–*е* – разнородные последовательности событий

Для любого набора событий расчет совместного распределения их вероятностей осуществляется по формулам (8) и (9).

Для варианта рис. 5, *а* – цепочки однородных событий – расчет производится по формуле (8):

$$P(\text{Кл}H_i У_i \mid S_i) = \frac{P(\text{Кл}H_i, S_i, У_i)}{P(S_i)} =$$

$$= \frac{P(\text{Кл}H_i)(S_i \mid \text{Кл}H_i)P(У_i \mid S_i)}{P(S_i)} =$$

$$= P(\text{Кл}H_i У_i \mid S_i)P(У_i \mid S_i). \quad (8)$$

Прочтение формулы позволяет вывести утверждение, что вероятность того, что нарушитель КлН$_i$ сможет реализовать УБИ способом S_i, зависит от вероятности наличия актуальной для S_i уязвимости $У_i$.

Для варианта рис. 5, *в* – цепочки разнородных событий – расчет производится по формуле (9):

$$P(TM_i И_i \mid У_i) = \frac{P(TM_i, У_i, И_i,)}{P(У_i)} =$$

$$= \frac{P(TM_i)(У_i \mid TM_i)P(И_i \mid У_i)}{P(У_i)} = P(TM_i \mid У_i)P(И_i \mid У_i). \quad (9)$$

Утверждение для цепочки событий ИБ на рис. 5, *в*: вероятная эффективность *ТМ* будет зависеть от вероятности наличия незакрытой уязвимости объекта ДВ.

Для цепочек последовательных событий на рис. 5, *б–е* формулы и утверждения о вероятностных зависимостях событий ИБ составляются аналогично приведенным выше примерам.

Рассмотрим взаимное влияние событий ИБ деструктивного и защитного характера представленных в виде сходимых цепочек (рис. 6).

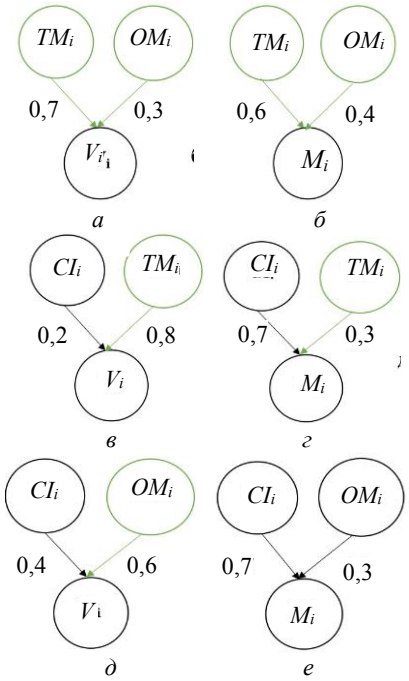

Рис. 6. Виды сходимых цепочек событий

Расчет их совместного распределения вероятностей для варианта рис. 6, *а* может быть произведен по формуле (10):

$$P(TM_i, OM_i, У_i) = \sum_{У_i} P(TM_i)P(OM_i)P(У_i \mid OM_i, TM_i) =$$

$$= P(OM_i \mid У_i)P(TM_i \mid У_i). \quad (10)$$

Утверждение для цепочки расходимых событий ИБ на рис. *б, а*: вероятность актуальности уязвимости $У_i$ будет зависеть от вероятностей ее ликвидации с помощью ОМ$_i$ и (или) ТМ$_i$.

Для цепочек последовательных событий на рис. 5, *е* и рис. 6, *а*, *б* формулы и утверждения о вероятностных зависимостях событий ИБ составляются в соответствии с приведенным примером (10).

Взаимное влияние деструктивных воздействий и МЗИ в виде цепочек расходимых событий представлено на рис. 7.

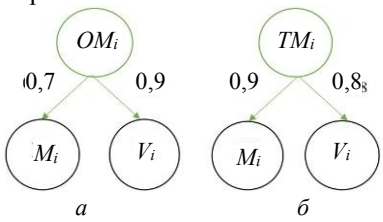

Рис. 7. Виды расходимых цепочек событий

Совместное распределение вероятностей для сходимой последовательности событий ИБ рассчитывается по формуле (11):

$$P(S_i, У_i \mid TM_i) = \frac{P(TM_i, S_i, У_i)}{P(TM_i)} = P(S_i \mid TM_i)\, P(У_i \mid TM_i). \quad (11)$$

Утверждение для цепочки сходимых событий ИБ: вероятность актуальности уязвимости $У_i$ и возможности ее эксплуатации способом S_i будет зависеть от вероятностей их нейтрализации защитными мерами (рис. 7, *а* – *ОМ$_i$* и (или) рис. 7, *б* – *ТМ$_i$*).

Разработанная методика позволяет рассчитать изменения численных значений вероятности событий при возможном наступлении (свершении) других событий, т.е. в динамике рассчитывать вероятностные зависимости деструктивных и защитных.

Выводы и заключение

В представленной работе выполнена научная задача и получены следующие результаты.

Первым научным вкладом стал предложенный подход, связанный с декомпозицией элементов распределенной информационной системы по уровням модели MBOC/ISO и определением объектов (концептов) ДВ на каждом из этих уровней. Это позволяет выявить уязвимости каждого концепта, определить точки входа и пути распространения УБИ и, следовательно, сформировать векторы тактик и сценариев их реализации.

Следующим научным вкладом стала разработка онтологической структурно-функциональной модели ТИМ РИС, интегрированной с вероятностной нейро-байесовской моделью. Такая интеграция двух разнотипных моделей стала возможной благодаря выявленным в ходе исследования свойствам симметричности структуры элементов РИС, реализуемых ими процессов и событий ИБ различного генеза. Это позволило получить новое качество интегрированной модели – возможность оценивать зависимости вероятностей исправного функционирования процессов в ТИМ РИС от реализации событий ИБ.

Разработанные и примененные в модели типовые информационные модули и типовые кластеры вероятностей событий информационной безопасности обеспечивают свойства универсальности и масштабируемости модели.

Предложенные методики позволяют определять степень критичности для РИС объектов ДВ, их уязвимостей, векторы атак и векторы защитных мер. В результате мы получаем технологическую карту состояния безопасности РИС или ее элемента.

Первичный расчет вероятностей событий ИБ деструктивного и защитного характера (их весов) может быть произведен с применением метода и программного продукта PROMETHEE-SAPEVO-M1.

В динамике оперативного управления их перерасчет осуществляется с применением формул Байеса для последовательных, сходящихся и расходящихся цепочек событий. Предлагаемый для использования алгоритм обучения НБМ позволяет проводить расчеты взаимных вероятностей событий ИБ.

Направлением дальнейших исследований в данной области будут разработка методик, реализующих формализованные алгоритмы определения сценариев, тактик и техник реализации УБИ и определения их предпочтительности для складывающейся ситуации. Также интересной будет разработка баз данных и баз знаний для обучения НБМ с применением предлагаемого варианта алгоритма AutoAI и расширение области применения методики и программного продукта PROMETHEE-SAPEVO-M1 в разработанной СППР.

Практическая значимость результатов исследования заключается в их использовании в деятельности организаций, осуществляющих проведение аттестаций РИС. Применение результатов исследования позволяет значительно сократить сроки проведения работ по формированию модели УБИ и повысить показатели обоснованности принятых решений и достоверности результатов оценки защищенности ТИМ РИС.

Работа выполнена в рамках реализации программы ЛИЦ «Доверенные сенсорные системы» (договор № 009/20 от 10.04.2020) при финансовой поддержке Минкомсвязи России и АО «РВК». Идентификатор соглашения о предоставлении субсидии – 0000000007119P190002.

Литература

1. A multi-criteria and statistical approach to sup–port the analysis of the superiority of OECD countries / D.A. De Moura Pereira, M. Dos Santos, I.P. De Araujo Costa, M.A.L. Moreira, A.V. Terra, S. De Souza Rocha, K. F. S. Gomez // IEEE Access: Interdisciplinary Open Access, VOLUME 10, 2022 [Электронный ресурс]. – Режим доступа: https://ieeexplore.ieee.org/document/9810236, свободный (дата обращения: 20.06.2022).

2. Gomez L. Multicriteria ranking with ordinal data / L. Gomez, A.-R. Muri, K.F.S. Gomez // Syst. Anal. – 1997. – Vol. 27, No. 2. – P. 139–146.

3. Multi-criteria analysis applied to the selection of aircraft by the Brazilian Navy / S.M.N. Maeda, I.P.A. Costa, M.A.P. Castro Junior, L.P. Favero, A.P.A. Costa, H.V.P. Corrisa, K.F.S. Gomez, M. Santos. – Prodution [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/353776847, свободный (дата обращения: 20.06.2022).

4. Баранов В.В. Св-во о гос. регистрации программы для ЭВМ № 2022665542 «Информационная система поддержки принятия решений при разработке системы защиты информации» (ИС ППР РСЗИ). Дата поступления: 12 августа 2022 г. Дата государственной регистрации в Реестре программ для ЭВМ: 17 августа 2022 г.

5. Международный стандарт ISO/IEC 15408-3:2022. Информационная безопасность, кибербезопасность и защита конфиденциальности – Критерии оценки ИТ-безопасности. – Ч. 3: Компоненты обеспечения безопасности [Электронный ресурс]. – Режим доступа: https://www.iso.org/home.html, свободный (дата обращения: 08.06.2022).

6. Международный стандарт ISO/IEC 27000. Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Обзор и словарь [Электронный ресурс]. – Режим доступа: https://pqm–online.com/assets/files/pubs/translations/std/iso-mek-27000-2016.pdf, свободный (дата обращения: 08.06.2022).

7. Методический документ. Утвержденная ФСТЭК России 5 февраля 2021 г. «Методика оценки угроз информационной безопасности» [Электронный рессурс]. – Режим доступа: https://fstec.ru/ tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g, свободный (дата обращения: 08.06.2022).

8. Key concepts of a systemological approach to adaptive monitoring of information security CPS / M. Poltavtseva, A. Shelupanov, D. Bragin, D. Zegda, E. Alexandrova // Symmetry. – 2021. – Vol. 13 (12). – P. 2425.

9. Industrial cyber-physical systems: risks assessment and attacks modeling / A.G. Kravets, N. Salnikova, K. Dmitrenko, M. Lempert. – 2020. – Vol. 260. – P. 197–210.

10. Стандарт ISO/IEC. 7498-1. Информационные технологии. Базовая эталонная модель: Базовая модель [Электронный рессурс]. – Режим доступа: https://www.ecma-international.org/wp-content/uploads/ s020269e.pdf, свободный (дата обращения: 12.06 2022).

11. Рассел С. Искусственный интеллект: современный подход: пер. с англ. / С. Рассел, П. Норвиг. – 2-е изд. – М.: ИД «Вильямс», 2016. – 1408 с.

12. Джиарратано Д. Экспертные системы: принципы разработки и программирования. – 4-е изд.; пер. с англ. – М.: ИД «Вильямс», 2007. – 1147 с.

13. Maksimova E. Prediction of destructive harmful effects on the object of critical information infrastructure / E. Maksimova, V. Baranov // Communications in Computer and Information Science book series (CCIS). – 2021. – Vol. 1395. – P. 88–99. DOI: 10.1007/978-981-16-1480-4_8.

14. Массель Л. Интеллектуальные инструменты поддержки для принятия стратегических решений по развитию интеллектуальных сетей / Л. Массель, А. Массель. – Вебсайт конференций E3S. – 2018 [Электронный рессурс]. – Режим доступа: https://doi.org/10.1051 /e3sconf/20186902009, свободный (дата обращения: 08.06 2022).

15. Скворцов Н.А. Вопросы согласования разнородных онтологических моделей и онтологических контекстов. Онтологическое моделирование / под ред. Л.А. Калиниченко: матер. семинара. – М.: ИПИ РАН, 2008. – С. 149–166.

16. Перл Д. Лаборатория когнитивных систем Калифорнийского университета. – Лос-Анджелес, Байесовские сети. – М.: Мир, 2000. – 102 с.

17. Azar A.T. Adaptive neuro-fuzzy systems. Fuzzy systems. – IN-TECH, Austria, 2010. – P. 85–110.

18. Ficilis P. Software project management technologies: an overview / P. Ficilis, V. Gerogiannis, L. Anthopoulos // Jour-

nal of Software and Application Development. – 2014. – P. 1096–1110.

19. Herzog A. Ontology of Information Security. International Journal of Information Security and Con-fidentiality. – 2007. – Vol. 1 (4). – P. 1–23.

20. Jaxen F. Bayesian networks and decision-making graphs. – M.: Sprinnger, 2001. – P. 54–120.

21. Singhal A. Security risk analysis of corporate networks using probabilistic attack graphs. Network security indicators. – Cham, 2017. – P. 53–73.

22. Egoshin N.S. Model of threats to the confidentiality of information processed in cyberspace, based on the model of information flows / N.S. Egoshin, A.N. Konev, A.N. Shelupanov // Symmetry. – 2020. – Vol. 12, iss. 11. – P. 1–18.

23. Катасёв А.С. Нейронечеткая модель формирования правил классификации как эффективный аппроксиматор объектов с дискретным выходом // Кибернетика и программирование. – 2018. – № 6. – С. 110–122.

24. PROMETHEUS-SAPEVO-M1 Hybrid approach based on ordinal and cardinal input data: multi-criteria evaluation of helicopters to support operations of the Brazilian Navy / M.A.L. Moreira, I.P. de Araujo Costa, M.T. Pereira, M. dos Santos, K.F.S. Gomez, F.M. Muradas // Algorithms. – 2021. – Vol. 14, No. 140 [Электронный ресурс]. – Режим доступа: https:// doi.org/10.3390/a14050140, свободный (дата обращения: 22.06.2022).

25. Brans J.-P. The method of ranking the preferences of an organization: The PROMETHEE method for making decisions based on several criteria / J.-P. Brans, P. Vinke // Management. Science. – 1985. – Vol. 31, No. 6. – P. 647–656.

26. SAPEVO-M: a method of group multicriteria ordinal ranking / K.F.S. Gomez, M. dos Santos, L.F.H. de Souza de Barros Teixeira, A.M. Sanseverino, M.R.S. dos Barcelos // Pesquisa Operacional. – 2020. – Vol. 40, No. 40. – P. 1–23. DOI: 10.1590/0101–7438.2020.040.00226524.

27. PROMETHE-SAPEVO-M1 hybrid modeling proposal: Multi-criteria evaluation of unmanned aerial vehicles for use in naval warfare / M.L. Moreira, K.F.S. Gomez, M. dos Santos, M.S. dos Carmo, J.V.G.A. Araujo // Proc. Int. Joint Conference on Industrial Engineering and Operations Management. – 2020. – Vol. 337. – P. 381–393. DOI: 10.1007/978-3-030-56920-4_31.

28. Radanliev P. Improving the cybersecurity of the healthcare system with the help of self-optimizing and self-adapting artificial intelligence (Part 2) / P. Radanliev, D. De Ruhr // Healthcare technology. – 2022. – Vol. 12. – P. 923–929 [Электронный ресурс]. – Режим доступа: https://doi.org/ 10.1007/s12553-022-00691-6, свободный (дата обращения: 22.08.2022).

29. Robotic system for analyzing information systems and communication networks in the field of cybersecurity / V.V. Baranov, Yu.Yu. Gromov, O.S. Lauta, E.A. Maksimova, N.P. Sadovnikova, L.V. Tretyakova // Journal of Physics: Conference Series. International Conference on Information Technologies in Business and Industry, ITBI–2020. – Bristol, England, 2020. – P. 12–19.

30. Koryshev N. Building a fuzzy classifier based on the whale optimization algorithm for detecting network intrusions / N. Koryshev, I. Khodashinsky, A. Shelupanов // Symmetry. – 2021. – No. 13 (7). – P. 1211.

Баранов Владимир Витальевич
Канд. военных наук, доцент, зав. каф. информационной безопасности Южно-Российского государственного политехнического университета (НПИ) им. М.И. Платова
Просвещения ул., 132, г. Новочеркасск, Россия, 346428
Тел.: +7-928-100-05-98
Эл. почта: baranov.vv.2015@yandex.ru

Шелупанов Александр Александрович
Д-р техн- наук, профессор,
президент Томского государственного университета систем управления и радиоэлектроники
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7-813-929-40-80
Эл. почта: saa@tusur.ru

Baranov V.V., Shelupanov A.A

Cognitive model for assessing the security of information systems for various purposes

The paper substantiates the relevance of the development of a cognitive model for assessing the security of information systems for various purposes, designed to support decision-making by officials of information security management bodies, analyzes scientific papers and research in this area, formulates requirements for the functional capabilities of the model, investigates and identifies the most appropriate modeling tools, develops integrated ontological and neuro-Bayesian models typical clusters of information systems, tactics and techniques for the implementation of UBI through the vulnerabilities of objects of various levels of the ISO/OSI model, protective and attacking influences, allowing to identify such objects of influence, their current vulnerabilities and scenarios for the implementation of information security threats, to calculate the joint probability distribution of information security events of various genesis, as well as to simulate the process of operational management of information security

Keywords: ontological model; neuro-Bayesian model, impact objects, vulnerabilities, structural survivability, functional survivability, information security measures.
DOI: 10.21293/1818-0442-2022-25-4-88-100

References

1. De Moura Pereira D.A., Dos Santos M., De Araujo Costa I.P., Moreira M.A.L., Terra A.V., De Souza Rocha S., Gomez K.F.S. A multi-criteria and statistical approach to support the analysis of the superiority of OECD countries. IEEE Access: Interdisciplinary Open Access, Vol. 10, 2022. Available at: https://ieeexplore.ieee.org/document/9810236, free (Accessed: June 20, 2022).

2. Gomez L., Muri A.-R., Gomez K.F.S. Multicriteria ranking with ordinal data. *System Analysis*, 1997, vol. 27, no. 2, pp. 139–146.

3. Maeda S.M.N., Costa I.P.A., Castro Junior M.A.P., Favero L.P., Costa A.P.A., Corrisa H.V.P., Gomez K.F.S., Santos M. Multi-criteria analysis applied to the selection of aircraft by the Brazilian Navy. Prodution, Available at: https://www.researchgate.net/publication/ 353776847, free (Accessed: June 20, 2022).

4. Certificate of state registration of the computer program № 2022665542 «Information system for decision making support in the development of an information security system» (IS PPR RSSI). V.V. Baranov, Received date August 12, 2022. Date of state registration in the Register of computer programs on August 17, 2022.

5. International standard ISO/IEC 15408-3:2022. Information Security, Cybersecurity and Privacy Protection – IT Security Assessment Criteria. Part 3: Security Components. Available at: https://www.iso.org/ home.html, free *(*Accessed: June 20, 2022) (in Russ.)

6. International Standard ISO/IEC 27000 Information Technology – Security methods – Information security management systems – Overview and dictionary. Available at: https://pqm-online.com/assets/files/pubs/translation/STD/ISO-

IEC-27000-2016.PDF format, free (Accessed: June 20, 2022) (in Russ.)

7. Methodological document. Approved by the FSTEC of Russia on February 5, 2021, Methodology for assessing threats to information security. Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/doku-menty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g, free. (Accessed: June 20, 2022). (In Russ.)

8. Poltavtseva M., Shelupanov A., Bragin D., Zegda D., Alexandrova E. Key concepts of a systemological approach to adaptive monitoring of information security CPS. *Symmetry*, 2021, vol. 13 (12), p. 2425.

9. Kravets A., N. Salnikova, K.Dmitrenko, M. Lempert. Industrial cyber-physical systems: risk assessment and attack modeling. *Research in the field of systems, decision-making and control*. 2020, vol. 260, pp. 197–210 (in Russ.)

10. ISO/IEC. 7498-1 STANDARD Information technologies. Basic Reference Model: Basic model [Electronic resource]. Available at: https://www.ecma-international.org/wp-content/uploads/s020269e.pdf, free (Accessed: June 12, 2022) (in Russ.)

11. Russell S., Norvig P. Artificial intelligence: a modern approach. Second Edition. USA, New Jersey, Pirson Education, 1995. 1043 p. (in Russ.).

12. Giarratano D. Expert Systems: Principles and Programming. 3rd Edition. USA, MA, Boston, PWS Publishing, 1998, 288 p.

13. Baranov V., Maksimova E. Prediction of destructive harmful effects on the object of critical information infrastructure. *Communications in Computer and Information Science Book Series (CCIS*), 2021, vol. 1395, p. 88–99. DOI: 10.1007/978-981-16-1480-4_8.

14. Massel L., Massel A. Intelligent support tools for making strategic decisions on the development of intelligent networks. *E3S Conference website successfully 2018.* Available at: https://doi.org/10.1051 /e3sconf/20186902009, free (Accessed: June 08, 2022) (in Russ.)

15. Skvortsov N.A. Issues of coordination of different ontological models and ontological contexts. Ontological modeling. *Edited by L.A. Kalinichenko: Materials of the seminar. M.: IPI RAS*. 2008, pp. 149–166 (in Russ.)

16. Pearl D. Laboratory of Cognitive Systems, University of California, Los Angeles. Bayesian Networks. *Moscow: Mir*, 2000, 102 p. (in Russ.)

17. Azar A.T. Adaptive neuro-fuzzy systems. Fuzzy systems. *IN-TECH, Austria*, 2010, pp. 85–110.

18. Ficilis P., Gerogiannis V., Anthopoulos L. Software project management technologies: an overview. *Journal of Software and Application Development*, 2014, pp. 1096–1110.

19. Herzog A. Ontology of Information Security. *International Journal of Information Security and Confidentiality*. 2007, no. 1 (4). p. 1–23.

20. Jaxen F. Bayesian networks and decision-making graphs. *M.: Springer*, 2001, pp. 54–120.

21. Singhal A. Security risk analysis of corporate networks using probabilistic attack graphs. *Network Security Indicators. Cham*, 2017, pp. 53–73.

22. Egoshin N.S., Konev A.N., Shelupanov A.A. Model of threats to the confidentiality of information processed in cyberspace, based on the model of information flows. *Symmetry*, 2020, vol. 12, Issue 11, 1840, pp. 1–18.

23. Katasev A.S. A neuro-fuzzy model for the formation of classification rules as an effective approximator of objects with a discrete output. *Cybernetics and Programming*, 2018, no. 6, pp. 110–122 (in Russ.)

24. Moreira M.A.L., de Araujo Costa I.P., Pereira M.T., dos Santos M., Gomez K.F.S., Muradas F.M. PROMETHEUS-SAPEVO-M1 Hybrid approach based on ordinal and cardinal input data: multi-criteria evaluation of helicopters to support operations of the Brazilian Navy. *Algorithms*, 2021, vol. 14, no. 140. Available at: https:// doi.org/10.3390/a14050140, free (Accessed: June 20, 2022).

25. Brans J.-P., Vinke P. The method of ranking the preferences of an organization: The PROMETHEE method for making decisions based on several criteria. *Management. Science*, 1985 vol. 31, no. 6, pp. 647–656.

26. Gomez K.F.S., dos Santos M., de Souza de Barros Teixeira L.F.H., Sanseverino A.M., dos Barcelos M. R. S. SAPEVO-M: a method of group multicriteria ordinal ranking. *Pesquisa Operacional*, 2020, vol. 40, no. 40, pp. 1–23, DOI: 10.1590/0101-7438.2020.040.00226524.

27. Moreira M.L., Gomez K.F.S., dos Santos M., dos Carmo M.S., Araujo J.V.G.A. PROMETHE-SAPEVO-M1 hybrid modeling proposal: Multi-criteria evaluation of unmanned aerial vehicles for use in naval warfare. *Proceedings of International. Joint Conference on Industrial Engineering and Operations Management*, 2020, vol. 337, pp. 381–393, DOI: 10.1007/978-3-030-56920-4_31.

28. Radanliev P., De Ruhr D. Improving the cybersecurity of the healthcare system with the help of self-optimizing and self-adapting artificial intelligence (Part 2). *Healthcare Technology*, 2022, vol. 12, pp. 923–929. Available at: https://doi.org/10.1007/s12553-022-00691-6, free (Accessed: August 22, 2022).

29. Baranov V.V., Gromov Yu.Yu., Lauta O.S., Maksimova E.A., Sadovnikova N.P., Tretyakova L.V. Robotic system for analyzing information systems and communication networks in the field of cybersecurity. *Journal of Physics: Conference Series. International Conference on Information Technologies in Business and Industry, ITBI-2020. Bristol, England*, 2020, pp. 12–19.

30. Koryshev N., Khodashinsky I., Shelupanov A. Building a fuzzy classifier based on the whale optimization algorithm for detecting network intrusions. *Symmetry*, 2021, vol. 13 (7), p. 1211.

Vladimir V. Baranov
Candidate of Military Sciences, Associate Professor,
Head of the Department of «Information Security»,
South Russian State Polytechnic University (NPI)
named after M.I. Platov
132, Prosveshcheniya str., Novocherkassk, Russia, 346428
Phone: +7-928-100-0-598
Email: kaf-ib@npi-tu.ru

Aleksandr A. Shelupanov
Doctor of Science in Engineering, Professor,
President of Tomsk State University of Control Systems
and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7-813-929-40-80
Email: saa@tusur.ru