ISSN 2658-5014 (Print) СИИТ ISSN 2686-7044 (Online)
2023. Т. 5, № 4 (13). С. 50–76 http://siit.ugatu.su
СИСТЕМНАЯ ИНЖЕНЕРИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.056.5 DOI 10.54708/2658-5014-SIIT-2023-no3-p50

Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных

А. М. Вульфин

Аннотация. В статье представлен обзор результатов исследования многоуровневой распределенной информационно-управляющей системы – объекта критической информационной инфраструктуры (КИИ), включая средства защиты информации с инструментами координации, стратегического целеполагания, распределения ресурсов и принятия решений. Предмет исследования – модели и методы комплексной оценки рисков информационной безопасности (ИБ) в составе процесса управления рисками ИБ объектов КИИ на основе методов интеллектуального анализа данных и технологий когнитивного моделирования. Цель – повышение достоверности и оперативности технологий и процедур комплексной оценки рисков ИБ объектов КИИ на основе методологии когнитивного моделирования и методов машинного обучения. Для достижения этой цели поставлены и решены следующие задачи: 1. Системный анализ проблемы комплексной оценки рисков ИБ объектов КИИ, выработка концепции ее решения. 2. Разработка проблемно-ориентированных моделей параметризации угроз и уязвимостей объектов КИИ. 3. Разработка и исследование метода и алгоритмов качественной оценки рисков ИБ объектов КИИ на основе технологий семантического анализа текстовых описаний угроз и уязвимостей. 4. Разработка и исследование метода и алгоритмов количественной оценки рисков ИБ объектов КИИ на основе когнитивного моделирования. 5. Разработка и исследование метода и алгоритмов оценки рисков ИБ объектов КИИ на основе выявления аномалий их состояния с помощью интеллектуального анализа временных рядов. 6. Разработка архитектуры исследовательского прототипа интеллектуальной системы поддержки принятия решений (ИСППР) по оценке рисков ИБ объектов КИИ и анализ результатов применения ИСППР при решении ряда прикладных задач по оценке уровня защищенности конкретных промышленных объектов и организаций.

Ключевые слова: информационная безопасность; интеллектуальный анализ данных; когнитивное моделирование; машинное обучение; аномалии; сетевые атаки; когнитивные атаки; семантический анализ.

Введение

Одним из непременных условий построения эффективной цифровой экономики является обеспечение надежной и безопасной работы современных промышленных предприятий и информационно-телекоммуникационных систем. Непрерывно возрастает сложность киберфизических систем, информационно-управляющих систем промышленных объектов, цифровых АСУ технологическими процессами топливно-энергетического комплекса, информационных систем финансового сектора и др. [1]. В то же время, как показывает статистика последних лет [2, 3], существенно возросло число случаев, связанных с попытками или успешной реализацией целенаправленных атак на подобные системы, в том числе объекты критической информационной инфраструктуры (КИИ). Согласно федеральному закону «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ [4], объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры. Глубокое проникновение промышленного Интернета в критическую инфраструктуру и производственный сектор привело к возрастанию тяжести последствий реализации подобных атак. Согласно мнению специалистов, ущерб от

кибератак на топливно-энергетическую отрасль достигает в среднем 13,2 млн долларов ежегодно, ожидаемый мировой ущерб от киберпреступлений в 2022 г. составит 9 млрд долларов, также отмечается, что повышение рисков информационной безопасности (ИБ) вынуждает к выработке общих подходов к обеспечению ИБ. Совершенствующаяся нормативно-правовая база в сфере ИБ объектов КИИ и действия регуляторов обусловливают необходимость разработки адекватных новым условиям научно обоснованных моделей, методов и инструментальных средств поддержки принятия решений при управлении рисками ИБ. На сегодняшний день масштабируемой и переносимой методологии не предложено. Согласно Государственной программе «Цифровая экономика Российской Федерации» от 28.07.2017 г. [5], в условиях роста угроз ИБ актуальными являются разработка и совершенствование моделей, методов и средств оценки рисков ИБ на основе анализа структурированных и слабоструктурированных данных для обеспечения устойчивости объектов КИИ на всех уровнях информационного пространства.

Степень разработанности темы и обсуждение решаемой задачи

Исследованиям в области управления рисками ИБ посвящены работы таких российских и зарубежных ученых, как Т. З. Аралбаев, И. М. Ажмухамедов, И. В. Аникин, А. С. Боровский, Т. И. Булдакова, В. И. Васильев, М. Б. Гузаиров, А. С. Катасёв, И. В. Котенко, О. Б. Макаревич, И. В. Машкина, Р. В. Мещеряков, Н. Г. Милославская, А. Г. Остапенко, О. Н. Чопоров, А. А. Шелупанов, A. Ajith, A. Jaquith, F. Massacci , S. Noel, J. L. Salmeron и др. Рассмотрены общие вопросы реализации риск-ориентированного подхода к обеспечению ИБ сложных и критических информационных систем, проанализированы лучшие практики управления ИБ промышленных предприятий и корпоративных систем. В то же время сегодня нет общепринятых методик и подходов к оценке качественных и количественных показателей защищенности (уровня ИБ) объектов КИИ, обладающих многоуровневой иерархической архитектурой и многообразием применяемых ИТ, средств автоматизации управления и контроля технологических процессов (ТП), разветвленными системами телекоммуникаций и т. п. Существующие подходы [6 – 9] направлены, как правило, на решение частных задач защиты информации, отдельных слабосвязанных между собой направлений и технических решений, что затрудняет их применение для современных высокотехнологичных объектов КИИ.

Анализ существующих подходов [10, 11] показал, что решение этой проблемы возможно на основе комплексирования и адаптации методов интеллектуального анализа данных (ИАД) и технологий когнитивного моделирования. Разработка в рамках данного подхода научно обоснованной методологии (то есть совокупности образующих ее элементов – концепции, моделей, методов, алгоритмов и методик) оценки рисков ИБ в составе процесса управления рисками ИБ объектов КИИ позволит получить объективную оценку уровня защищенности этих объектов в условиях воздействия возможных внешних и внутренних угроз, оценить последствия (ущерб) от воздействия этих угроз и предложить адекватные защитные меры по снижению существующих (или потенциально возможных) рисков ИБ с учетом требований существующих нормативных документов. Применение методов ИАД должно обеспечить повышение оперативности и достоверности результатов комплексной оценки уровня защищенности объектов КИИ (рисков ИБ) с учетом имеющейся неопределенности, то есть неполноты и нечеткости исходной информации об угрозах, уязвимостях и последствиях возможных атак, наличия субъективных факторов при принятии решений об оценке рисков ИБ и выборе эффективных контрмер по защите объектов КИИ от воздействия злоумышленников и других деструктивных факторов. Известные публикации, связанные с оценкой рисков ИБ с помощью технологий ИАД и методов машинного обучения, касаются лишь отдельных аспектов, прежде всего, качественной оценки уровня защищенности и не допускают возможности их прямого распространения на задачи комплексной оценки рисков ИБ объектов КИИ.

Объектом данного исследования является многоуровневая распределенная информационно-управляющая система (объект КИИ), включая входящие в его состав средства защиты

информации с инструментами координации, стратегического целеполагания, распределения ресурсов и принятия решений. Предмет исследования – модели и методы комплексной оценки рисков ИБ в составе процесса управления рисками ИБ объектов КИИ на основе методов интеллектуального анализа данных и технологий когнитивного моделирования. Цель работы – повышение достоверности и оперативности технологий и процедур комплексной оценки рисков ИБ объектов КИИ на основе методологии когнитивного моделирования и методов машинного обучения. Для достижения этой цели поставлены и решены следующие задачи:

1. Системный анализ проблемы комплексной оценки рисков ИБ объектов КИИ, выработка концепции ее решения.
2. Разработка проблемно-ориентированных моделей параметризации угроз и уязвимостей объектов КИИ.
3. Разработка и исследование метода и алгоритмов качественной оценки рисков ИБ объектов КИИ на основе технологий семантического анализа текстовых описаний угроз и уязвимостей.
4. Разработка и исследование метода и алгоритмов количественной оценки рисков ИБ объектов КИИ на основе когнитивного моделирования.
5. Разработка и исследование метода и алгоритмов оценки рисков ИБ объектов КИИ на основе выявления аномалий их состояния с помощью интеллектуального анализа временных рядов.
6. Разработка архитектуры исследовательского прототипа интеллектуальной системы поддержки принятия решений (ИСППР) по оценке рисков ИБ объектов КИИ и анализ результатов применения ИСППР при решении ряда прикладных задач по оценке уровня защищенности конкретных промышленных объектов и организаций.

При решении поставленных задач использовались методы системного анализа, математического и когнитивного моделирования; методы семантического анализа, нейронных сетей и машинного обучения; методы оценки рисков ИБ, обнаружения аномалий временных рядов.

Анализ современного состояния в области комплексной оценки рисков ИБ объектов КИИ

Существующие подходы к анализу качественной и количественной оценки рисков ИБ объектов КИИ с использованием технологий интеллектуального анализа данных направлены, как правило, на решение частных задач, отдельных поддающихся анализу направлений и решений, что затрудняет их применение для современных высокотехнологичных объектов КИИ. В [12] предлагается концепция комплексной оценки рисков ИБ объектов КИИ с применением технологий нечеткого когнитивного моделирования и методов машинного обучения, заключающаяся в:

– проведении системного анализа проблемы безопасности киберфизических объектов в пределах единой информационной среды (киберпространства) и оценке потенциального ущерба (последствий) для физического мира и человека [13];

– автоматизации сбора и анализа индикаторов угроз из множества каналов (источников) и выявлении потенциальных угроз, уязвимостей и векторов атак на основе оценки семантической близости их текстовых описаний с возможностью ранжирования (присвоения уровня критичности) и приоритезации для последующего структурирования, консолидации и обогащения накопленной информации об уязвимостях информационной инфраструктуры и ее компонент, выявлении наиболее успешных сценариев реализации атак и оценки их последствий для объектов КИИ на основе взаимодействия с внешними базами знаний [14–16];

– автоматизации сбора и анализа статистических данных о событиях информационной безопасности с построением прямых связей между выявленными уязвимостями и угрозами безопасности информации для анализируемой информационной системы (объекта КИИ)

на основе методов анализа слабоструктурированных текстовых описаний и интеграцией с существующими банками данных об угрозах и уязвимостях программного и аппаратного обеспечения [17, 18];

– когнитивном моделировании [19] как средстве реализации системного риск-ориентированного подхода к количественной оценке рисков ИБ объекта КИИ путем построения иерархии вложенных когнитивных моделей в базисе интервальных чисел, с возможностью анализа различных сценариев воздействия внутренних и внешних злоумышленников и с учетом накопленных данных о состоянии объекта;

– получении оценок рисков ИБ объекта КИИ на основе обнаружения аномалий временных рядов накапливаемых параметров, характеризующих состояние объектов, сетевого трафика промышленных сетей и поведения пользователей конечных систем, основанных на построении нейросетевых моделей объекта и последующей оценке согласованности модельных данных и поведения объекта [20–23].

Разработка и исследование моделей параметризации множеств угроз и уязвимостей, приводящих к нарушению ИБ

В соответствии с рекомендациями ГОСТ 62443 [24] реализация системного риск-ориентированного подхода к обеспечению ИБ осуществляется на основе декомпозиции (сегментации) инфраструктуры объектов КИИ на относительно независимые выделенные локальные зоны безопасности и связывающие их тракты с учетом требований к уровню их безопасности.

Качественная и количественная оценка рисков ИБ объекта КИИ, согласно ГОСТ 27005 и 62443, базируется на трехфакторной формуле оценки рисков ИБ и определяется как произведение $C_{\text{ущ}_i}$ потенциального ущерба (последствия), наносимого i-ому информационному ресурсу выделенной зоны безопасности (в относительных единицах к ценности актива) на вероятность $P_{\text{угр}_j}$ возникновения j-й угрозы и вероятность $P_{\text{уязв}_k}$ использования k-й уязвимости: $R_i = P_{\text{угр}_j} P_{\text{уязв}_k} C_{\text{ущ}_i}$.

При оценке рисков ИБ необходимо определить целевые и достигнутые уровни безопасности, определяемые для каждой зоны безопасности, на основе анализа архитектуры объекта КИИ, идентификации и классификации активов, подлежащих защите, и параметризации угроз и уязвимостей. Следовательно, необходим иерархический комплекс моделей, позволяющих учитывать не только вероятность нарушения безопасности и ее проявления, но и оценивать эффективность контрмер, учитывать выявление новых уязвимостей, эволюцию угроз и методов атак – то есть эволюцию объекта защиты и необходимость уточнения оценок вероятностей реализации угроз и эксплуатации уязвимостей, а также реализацию опережающей стратегии защиты (проактивная защита), основанной на предсказании угроз (предиктивный анализ) и раннем обнаружении атак с целью адаптации системы к предполагаемому деструктивному воздействию. Предлагаемые модели должны обеспечивать агрегацию оценок рисков ИБ в пределах выделенных зон и возможность перехода к интегральным оценкам рисков ИБ для укрупненных зон анализа с возможностью выбора оптимального (рационального) способа защиты информации с учетом ограничений на величину рисков и выделяемых ресурсов на реализацию контрмер.

Для комплексной оценки риска ИБ объекта КИИ необходимо решение задач оценки состава потенциальных угроз ИБ, уязвимостей и сценариев реализации атак с возможностью их ранжирования по приоритетам (присвоения уровня критичности) и выбором рационального состава защитных мер. Для решения этих задач рекомендуется использовать существующие открытые базы знаний угроз (Threat Intelligence) и уязвимостей (Vulnerability Intelligence), которые содержат полученные из различных источников систематизированные текстовые описания аспектов безопасности программного и аппаратного обеспечения информационной

инфраструктуры, консолидированные в виде слабосвязанных групп иерархических гипертекстовых документов в отдельных базах данных (БДУ ФСТЭК России, CAPEC, ATT&CK, OWASP, STIX, WASC и др.).

Для автоматизации поиска и анализа баз знаний предложена модель параметризации и оценки семантической близости текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения объектов КИИ [15, 18] (рисунок 1).

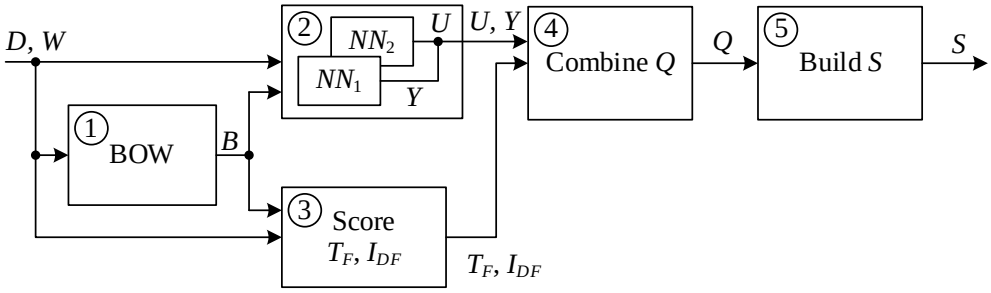


Рис. 1 Модель параметризации и оценки семантической близости текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения объектов КИИ: D – множество текстовых описаний; W – множество уникальных термов; B – разреженная матрица вхождений термов; NN_1, NN_2 – Word2Vec- и Doc2Vec-модели; U, Y – формализованные векторы вложений; Q – гетерогенный вектор признаков; S – разреженная матрица семантической близости; T_F, I_{DF} – статистическая мера оценки важности термов; BOW – словарь вхождений термов.

После предобработки текстовых описаний (D) и построения словаря W (множество уникальных термов) формируется разреженная матрица B (1) вхождений термов (w_i) в текстовое представление ($d_j \in D$). С помощью предобученных нейросетевых моделей NN_1 и NN_2 (2) строятся векторные вложения на уровне термов (Word2Vec) и на уровне текстовых описаний (Doc2Vec), которые позволяют сформировать гетерогенный вектор признаков (4) мультиязычного текстового описания с учетом (3) статистической меры оценки важности термов (T_F, I_{DF}). Выходом модели (5) является разреженная матрица S семантической близости текстовых описаний.

Применение модели позволяет сократить в 7–10 раз объемы просматриваемых экспертом данных и уменьшить в 10–12 раз время анализа при оценке опасности выявленных уязвимостей и релевантных им угроз нарушения ИБ с помощью префильтрации на основе технологий интеллектуального анализа текстов, тем самым повышая продуктивность работы специалиста.

В [25] предлагается модель количественной оценки степени опасности новых уязвимостей (рисунок 2), для которых экспертная оценка метрики CVSS (Common Vulnerability Scoring System 2 и 3 версии) еще не определена, на основе прогнозирования набора метрик с помощью анализа текстового описания. Предложены два подхода [25] для количественной оценки базовой метрики CVSS опасности уязвимостей по формализованному текстовому описанию: построение ансамбля предикторов для оценки отдельных значений набора метрик с последующим расчетом результирующего значения и построение ансамбля регрессоров для непосредственной количественной оценки результирующего значения метрики CVSS. Ансамбль моделей позволяет получить оценку метрик опасности уязвимости CVSS на уровне F_1 = 0,80–0,85 и оценку MSE = 0,865 для ансамбля регрессоров.

Для автоматизации низкоуровневого моделирования сценариев эксплуатации уязвимостей и реализации угроз на основе описания шаблонов компьютерных атак, содержащихся в базах знаний (БДУ ФСТЭК России, CAPEC, MITRE и ATT&CK), характеризующих различные аспекты безопасности программного и аппаратного обеспечения, предлагается семантическая модель текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения (рисунок 3) зоны объекта КИИ [16], в виде графа

$$G = \{V, E, D\},$$

где V – множество вершин графа – текстовые описания;

$$V = V_{CPE} \cup V_{CVE} \cup V_{CWE} \cup V_{CAPEC} \cup V_{Techs} \cup V_{Tackts} \cup V_{TO} \cup V_T,$$

E – множество взвешенных ориентированных ребер, устанавливающих отношения между текстовыми описаниями:

$$E \subseteq V \times V, \quad e(v_i, v_j), \quad v_i, v_j \in V,$$

$D(e)$ – функция, определяющая степень семантической близости для концептов $v_i, v_j \in V$.

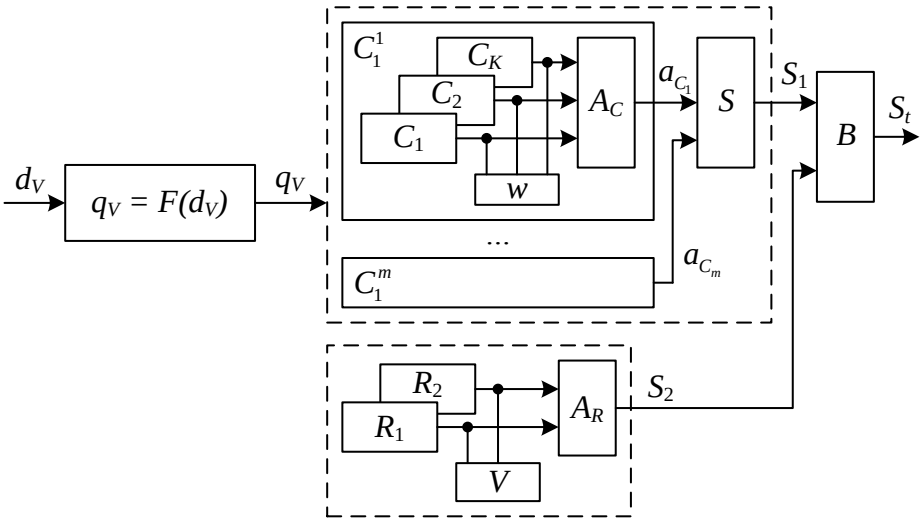


Рис. 2 Ансамбль моделей для прогнозирования базовой метрики оценки степени опасности уязвимости на основе формализованного текстового описания: d_V – текстовое описание уязвимости; q_V – формальный вектор признаков текстового описания; C – ансамбль моделей-классификаторов набора метрик; R – модели-регрессоры количественной оценки степени опасности уязвимости; A – модули согласования моделей ансамбля; w, v – весовые коэффициенты моделей в составе ансамбля; S – оценки степени опасности уязвимости; B – блок итоговой количественной оценки степени опасности уязвимости.

Модель позволяет формализовать логическую цепочку: «множество выявленных уязвимостей программного обеспечения → множество релевантных угроз → множество наиболее вероятных сценариев реализации угроз → возможные киберфизические последствия» с учетом требований нормативных документов ФСТЭК России. Использование модели позволяет снизить трудоемкость формирования перечня актуальных угроз и уязвимостей за счет префильтрации несвязанных или недостижимых вершин (угроз).

На этапе анализа сценариев реализации угроз с возможностью установки приоритетов мер по их устранению необходимо обеспечение видимости и контекста потенциальной атаки за счет агрегации и анализа данных из множества источников, характеризующих состояние подсистем объекта КИИ. В [1] предлагается модель обнаружения аномалий состояния объектов и сущностей в зоне анализируемого объекта КИИ (рисунок 4), основанная на применении методов машинного обучения и интеллектуального анализа собираемых данных мониторинга состояния объектов и сущностей в виде многомерных временных рядов.

Многомерные временные ряды (МВР) представляют собой последовательность измерений, собранных с датчиков в зоне безопасности объекта КИИ. Аномалии представляют собой отрезки временного ряда с соотнесенными событиями состояния объекта. Применение адаптивного оконного анализа [26, 27] позволяет выделять непрерывные подпоследовательности

ВР, для которых выполняется процедура построения признакового описания на основе статистических функций, параметрических моделей, приближающих сегмент ВР, семейства регрессионных и нейросетевых авторегрессионных моделей.

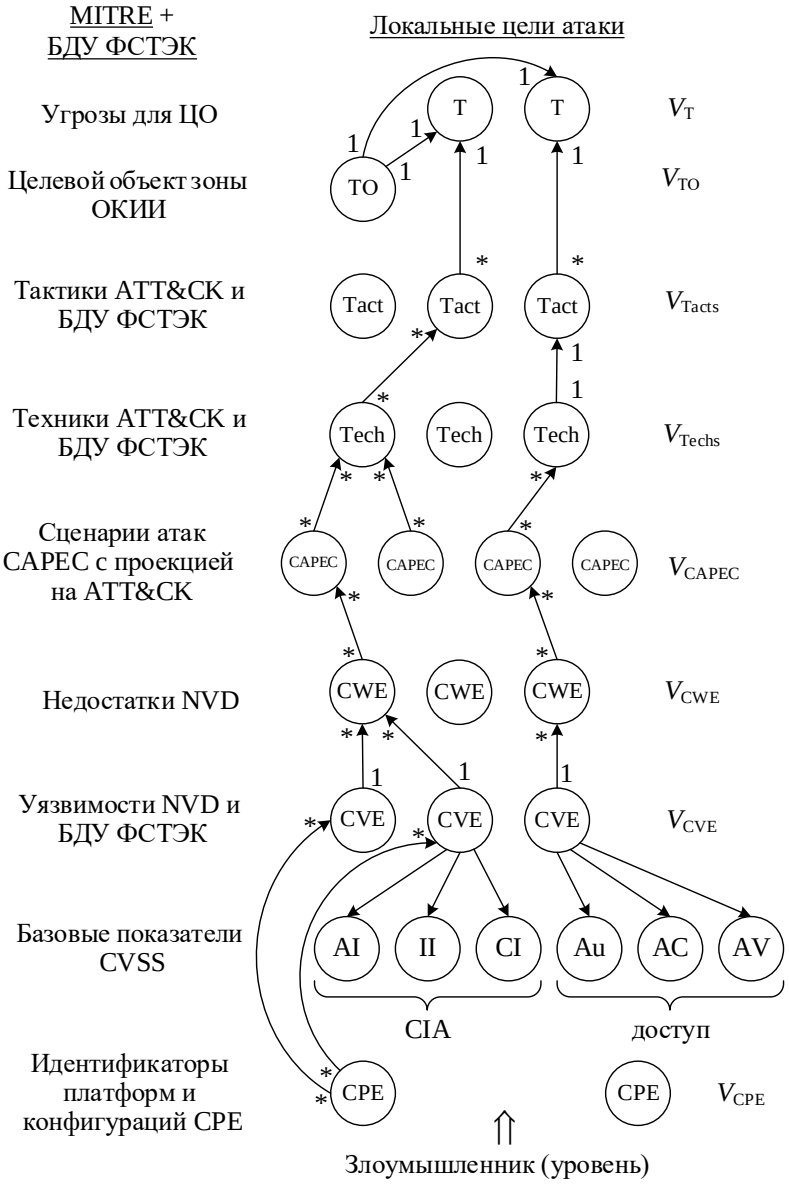


Рис. 3 Семантическая модель текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения объектов КИИ в задаче анализа актуальных угроз и уязвимостей: V_{CPE} – идентификаторы платформ и конфигураций для программно-аппаратного обеспечения; V_{CVE} – идентификаторы выявленных уязвимостей для каждого компонента; V_{CWE} – текстовые описания CWE, представляющие недостатки (слабые места) программного и аппаратного обеспечения; V_{CAPEC} – металшаблоны CAPEC, описывающие известные типовые атаки; V_{Techs} – техники реализации атаки, которые описывают инструменты, технологии, утилиты и т. д., используемые нарушителями; V_{Tackts} – тактики, то есть действия на разных этапах реализации атаки; V_{TO} – объекты воздействия; V_T – угрозы.

Гетерогенная модель ансамбля детекторов для обнаружения аномалий в МВР включает детекторы на основе нейросетевых автоенкодеров (NAE) с долгой-краткосрочной памятью (LSTM), модели оценки выбросов с автоподстройкой порога (LOF-детектор), модели обнаружения аномалий на основе изолирующего леса (IFO-детектор). Для создания модели обнаружения аномалий используются данные о штатном функционировании объекта или подсистемы для построения модели нормального функционирования либо имеющаяся модель (математическая, полунатурная). Модель может быть использована для обнаружения аномалий состояния объекта КИИ, пользователя конечной системы и пользовательского окружения объекта КИИ [1, 28–34].

Рис. 4 Модель обнаружения аномалий состояния подсистем в зоне объекта КИИ.

С целью параметризации и оценки угрозы нарушения конфиденциальности и целостности информации и оценки соблюдения требований политики ИБ объекта КИИ разработан комплекс моделей анализа поведения пользователей конечной системы [35–42] (рисунок 5), включающий построение цифрового отпечатка (ЦО) пользователя (модель пользовательского окружения конечной системы и модель динамического профиля взаимодействия пользователя с конечной системой); профилирование состояния пользователя.

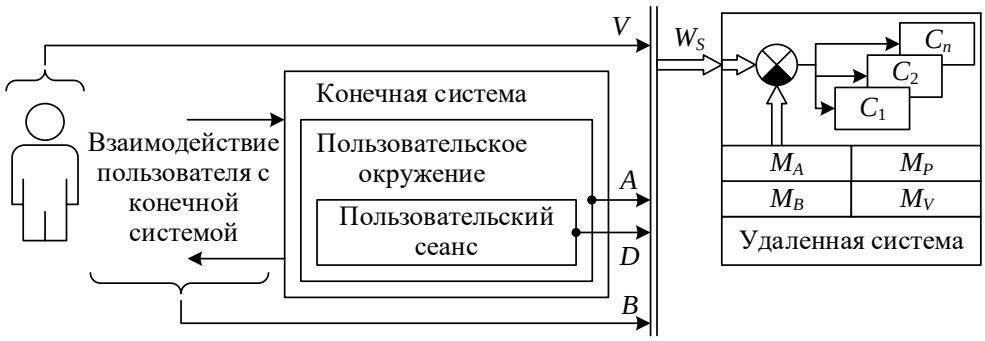


Рис. 5 Комплекс моделей обнаружения аномалий поведения пользователя и пользовательского окружения: *A* – ЦО пользовательского окружения при работе с Web-системой; *B* – ЦО динамических биометрических признаков пользовательского сеанса; *D* – ЦО динамического профиля пользователя (характер действий в удаленной системе); *V* – образ автоматического профилирования пользователя (видеоаналитика); *M* –модели обнаружения аномалий.

После параметризации и формирования перечня актуальных угроз и уязвимостей с помощью предложенных моделей для каждой из выделенных зон безопасности объекта КИИ осуществляется переход к построению и последующему анализу иерархии нечетких когнитивных карт с целью формирования обоснованной качественной и количественной оценки показателей рисков ИБ объекта КИИ.

В [8] используются когнитивные модели на основе традиционных нечетких когнитивных карт (НКК), нечетких продукционных когнитивных карт (НПКК), обобщенных интервально-значных НКК (серые и интуиционистские НКК).

НКК – это ориентированный граф, заданный с помощью кортежа множеств:

$$\text{НКК} = \langle C, F, W \rangle,$$

где $C = \{C_i\}$ – множество концептов, $F = \{F_k\}$ – множество направленных дуг графа, $W = \{W_{ij}\}$ – множество весов связей НКК, $X_i(t)$ – значение переменной состояния i-го концепта C_i в момент времени t, определяемое в общем случае уравнением

$$\tilde{X}_i(t+1) = f\left(\tilde{X}_i(t) \oplus \left(\sum_{\substack{j=1 \\ (j \neq i)}}^{n} \oplus \widetilde{W}_{ji} \otimes \tilde{X}_j(t)\right)\right), \ (i = 1, 2, \dots, n), \tag{2}$$

где веса связей $\widetilde{W}_i$ и переменные состояния $\tilde{X}_i(t)$ представляют собой интервальные числа, определяемые как элементы нечетких интервальных множеств, $\oplus$ и $\otimes$ – операции сложения и умножения интервальных чисел, заданные на нечетких интервальных множествах, f – нелинейная функция активации концепта.

В качестве основы для построения НКК использованы способы задания интервальных нечетких множеств: серые числа, интуиционистские числа. Под серым множеством $A \subseteq X$ понимается множество

$$A = \{< x, [\underline{x}, \overline{x}] > | x \in X\}, \tag{3}$$

элементами которого являются серые числа $x \in [\underline{x}, \overline{x}] \leq A$, $[\underline{x}, \overline{x}] \in [0,1]$, где $\underline{x}$ и $\overline{x}$ – нижняя и верхняя граница серого числа x, X – универсальное множество. Веса связей между концептами серой НКК задаются в виде серых чисел $[\underline{W}_{ij}, \overline{W}_{ij}]$; переменные состояния концептов – серые числа $[\underline{X}_i, \overline{X}_i]$.

В [8] рассмотрены особенности применения НПКК для решения задачи оценки рисков ИБ. Используется описание взаимодействия между концептами с помощью системы нечетких правил, отражающих знания и опыт экспертов предметной области. Предполагается, что переменная состояния X_i каждого концепта C_i рассматривается как лингвистическая переменная, принимающая значения из нечеткого терм-множества $\{T_{i1}, T_{i2}, \dots, T_{im}\}$, подмножества (термы) которого $T_{ik}, (k = 1,2, \dots, m)$, в свою очередь, задаются функциями принадлежности:

$$T_{ik} = (\mu_{ik}(X_i), X_i), \mu_{ik}: X_i \to [0,1],$$

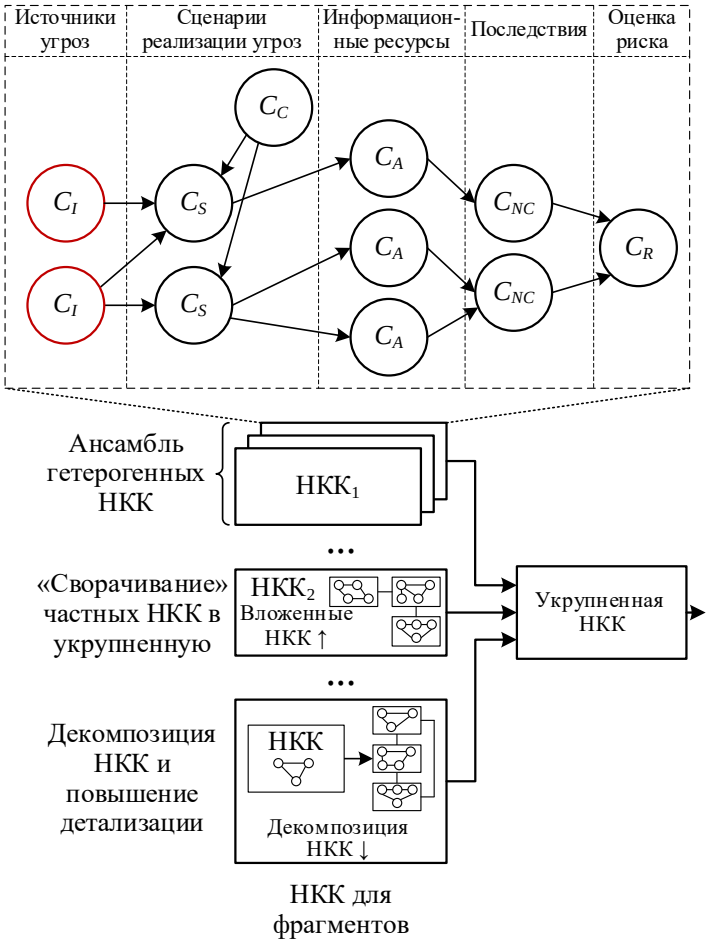
где $X_i \in [0,1]$ или $X_i \in [-1,1]$.

Предложена общая схема построения нечеткой когнитивной модели оценки рисков ИБ [43] (рисунок 6).

Разработка метода и алгоритмов комплексной оценки рисков ИБ объекта КИИ

На основе предложенной в работе модели оценки семантической близости текстовых описаний разработан метод ранжирования по приоритетам угроз с учетом зависимостей между угрозами и выявленными для каждой зоны безопасности объекта КИИ уязвимостями [15, 18] (рисунок 7).

Для реализации дивизимного (угроза и приводящие к ее реализации уязвимости) и агломеративного (от выявленных уязвимостей к релевантным угрозам) сопоставления устанавливается соответствие $F \subset T \times V$ между элементами множества угроз $T = \{T_1, T_2, \dots, T_l\}$ и множества уязвимостей $V = \{V_1, V_2, \dots, V_t\}$ на основе анализа матрицы S оценок семантической близости текстовых описаний.



1. Определение множества концептов, характеризующих:

1.1. C_{NC} – негативные последствия реализации угроз ИБ для объекта КИИ.

1.2. C_A – информационные ресурсы объекта КИИ.

1.3. C_I – источники угроз.

1.4. C_S – угрозы нарушения ИБ и сценарии их реализации (тактики и техники).

1.5. C_R – оценка риска ИБ.

1.6. C_C – выбор рационального способа защиты с учетом ограничений.

2. Оценка связей между концептами (F) и взаимовлияния концептов с помощью нечеткой лингвистической шкалы с возможностью учета разброса мнений экспертов (W).

3. Декомпозиция НКК и вложение частных НКК, построение ансамблей НКК для достижения требуемого уровня детализации представления.

4. Моделирование и количественная оценка рисков ИБ.

5. Выбор рационального способа и средств защиты объекта КИИ с учетом требований нормативной базы и имеющихся ограничений.

Рис. 6 Обобщенная схема построения нечеткой когнитивной модели оценки рисков ИБ объекта КИИ.

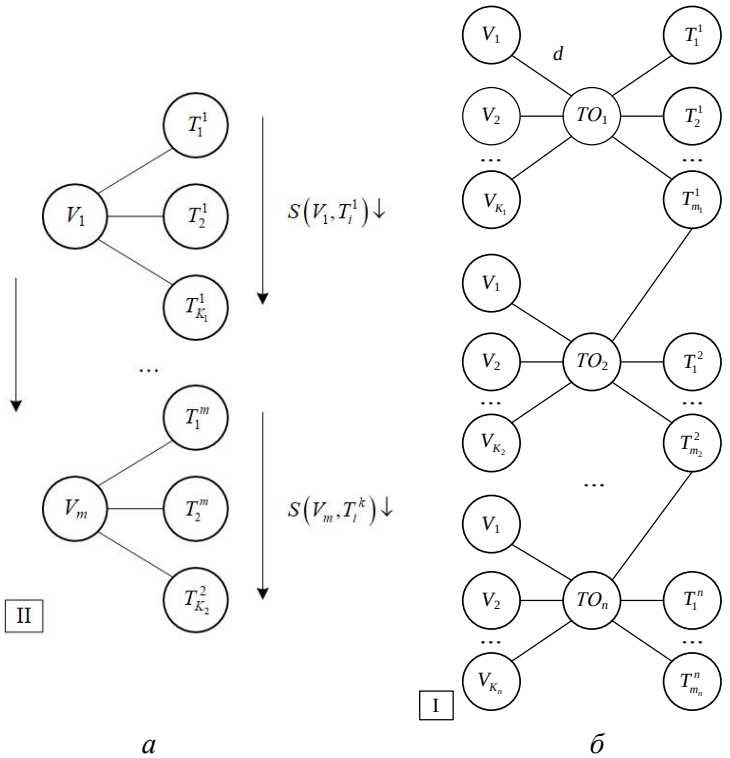


Рис. 7 Список актуальных уязвимостей, ранжированных по степени критичности, и сопоставленные с ними угрозы (в порядке убывания метрики семантической близости) (*а*); соотнесения множества угроз T и уязвимостей V через промежуточные узлы – объекты воздействия ТО (*б*) (ТО_j – объект воздействия, $j = \overline{1,n}$; Т_j^i – угроза, связанная с ТО_j; $i = \overline{1,m_j}$; V_{K_j} – уязвимость, связанная с ТО_j).

Пороговая фильтрация и экспертная корректировка разреженной матрицы позволяют для каждой зоны объекта КИИ построить группу актуальных уязвимостей, ранжированных по степени критичности, и сопоставленных с ними угроз (в порядке убывания метрики семантической близости), а также выполнить соотнесение множества угроз *T* и уязвимостей *V* через промежуточные узлы – объекты воздействия ТО.

В [17, 20] разработана архитектура конвейера по обработке текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения объекта КИИ (рисунок 8).

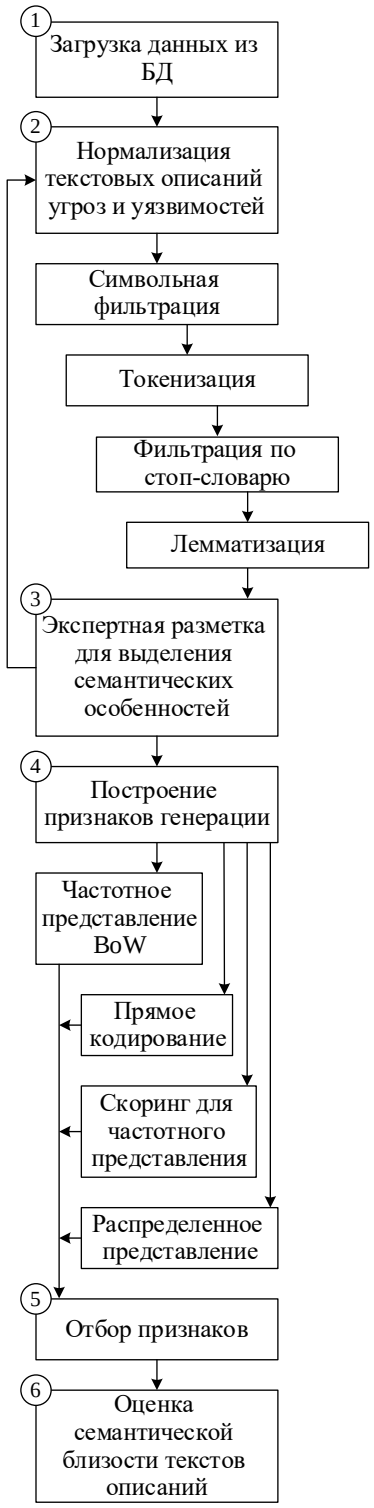


Рис. 8 Архитектура конвейера по обработке текстовых описаний:

1 – загрузка данных из локальной БД – преобразование текстовых полей в единое текстовое описание;

2 – нормализация текстовых описаний угроз и уязвимостей: символьная фильтрация, токенизация и фильтрация с использованием общего и специализированного (формируемого экспертами) «стоп-словарей» и лемматизация;

3 – экспертная структурно-семантическая разметка текста для выделения семантических особенностей текстовых описаний (ключевые слова, ключевые словосочетания, именованные сущности) и уточнение специализированного «стоп-словаря»;

4 – построение формализованного вектора признаков текстовых описаний. Применяемые схемы частотного представления (Bag of Word, BoW), прямого кодирования, скоринга для частотного представления (BoW + TF-IDF) и распределенного представления (с помощью нейросетевых моделей векторных вложений Word2Vec, Doc2Vec) позволяют сформировать гетерогенный вектор признаков текстового описания;

5 – отбор наиболее значимых признаков с помощью экспертной оценки структуры двухмерной визуализации стохастического вложения соседей с *t*-распределением (TSNE), редуцированного пространства признаков с помощью метода главных компонент (PCA) или приближения и проекции однородного многообразия (UMAP);

6 – оценка семантической близости текстовых описаний и формирование матрицы попарных расстояний на основе оценки косинус-меры сходства гетерогенный вектор признаков текстового описания.

С целью автоматизации сбора индикаторов угроз из множества каналов (источников) и выявления потенциальных угроз, уязвимостей и векторов атак с возможностью их ранжирования (присвоения уровня критичности) для последующего структурирования, выявления наиболее опасных сценариев реализации атак и оценки их последствий на основе предложенных моделей и метода разработана автоматизированная система анализа угроз и уязвимостей объекта КИИ на основе технологий семантического анализа их текстовых описаний [15, 18]. Система позволяет автоматизировать сбор и обработку накапливаемых с помощью сканеров безопасности данных об обнаруженных уязвимостях. Основной модуль системы реализует метод интеллектуального анализа текстовых описаний аспектов безопасности программного и аппаратного обеспечения информационной инфраструктуры. Применение данной системы позволяет осуществить ранжирование по приоритетам угроз с учетом зависимостей между угрозами и выявленными уязвимостями.

Структура системы анализа угроз и уязвимостей объекта КИИ включает в себя следующие основные подсистемы (рисунок 9):

– подсистему локального хранения актуальной копии БДУ ФСТЭК России (I);

– подсистему сопоставления угроз и уязвимостей на основе их текстового описания (II);

– подсистему оценки актуальных угроз и уязвимостей для сегмента информационной инфраструктуры (III).

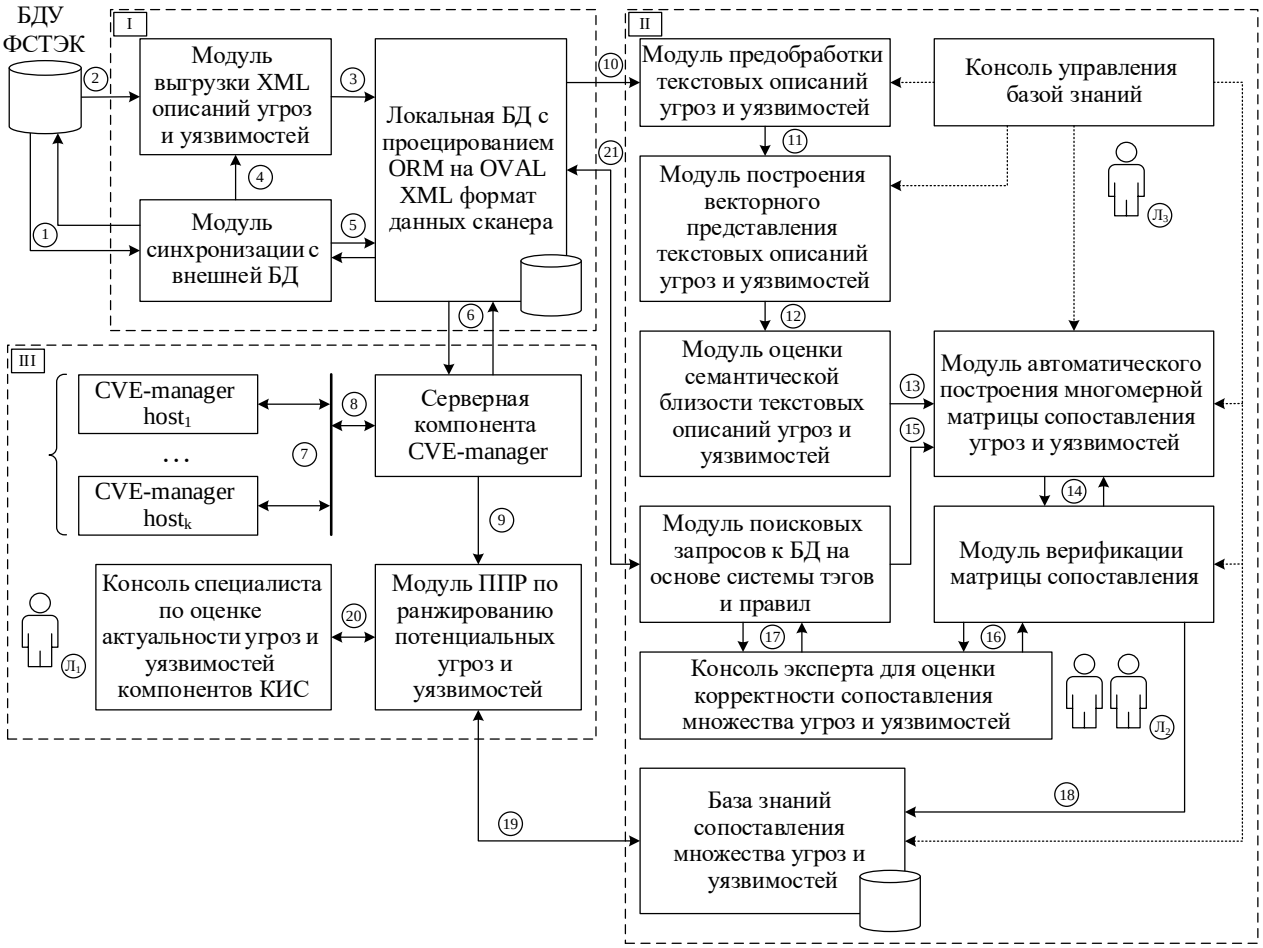


Рис. 9 Структурно-функциональная организация системы анализа актуальных угроз и уязвимостей на основе оценки семантической близости их текстовых описаний.

Применение системы позволяет:

– автоматизировать процесс сопоставления и ранжирования угроз ИБ для каждой выявленной уязвимости на рабочих станциях и серверах информационной инфраструктуры;

– снизить когнитивную нагрузку на эксперта, и повысить достоверность оценки степени опасности уязвимостей ПО за счет использования дополнительной информации о существующих зависимостях между выявленными уязвимостями и потенциальными угрозами;

– масштабировать решение за счет интеграции с существующими БД уязвимостей и формализации знаний экспертов о прецедентах сопоставления угроз и уязвимостей в пополняемой базе.

В [25] разработана структура системы оценки степени опасности уязвимостей на основе прогнозирования набора метрик CVSS с помощью анализа текстового описания для повышения точности и оперативности оценки (рисунок 10).

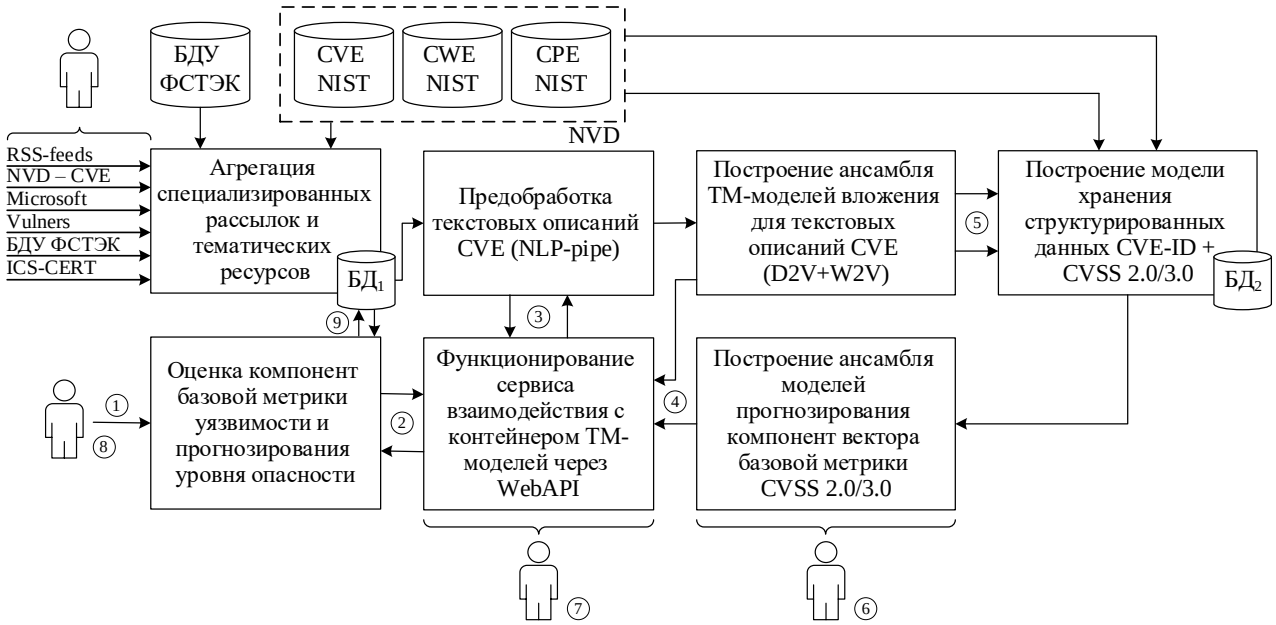


Рис. 10 Структура системы оценки степени опасности уязвимостей на основе интеллектуального анализа данных.

Первый этап работы системы связан со сбором и агрегацией специализированных новостных рассылок и тематических ресурсов в виде слабоструктурированных текстовых данных для построения документо-ориентированной БД.

Практическая значимость системы обусловлена повышением точности и оперативности оценки метрик опасности уязвимостей с возможностью интеграции в систему аудита и инвентаризации для оперативного принятия мер защиты от новых уязвимостей. Предложена методика оценки актуальных угроз и уязвимостей программного обеспечения объекта КИИ с использованием методов семантического анализа текстовых описаний. Завершающий этап предлагаемой методики позволяет перейти к построению когнитивной модели оценки рисков ИБ для объектов КИИ. Автоматизированное моделирование и оценка актуальности угроз и сценариев их реализации на основе перечня выявленных уязвимостей для всех компонентов КИИ позволяют выявить наиболее вероятные сценарии реализации угроз и оценить последствия от их реализации.

Для реализации предложенной методики разработана система построения и анализа семантической модели текстовых описаний объектов зоны безопасности объекта КИИ (рисунок 11).

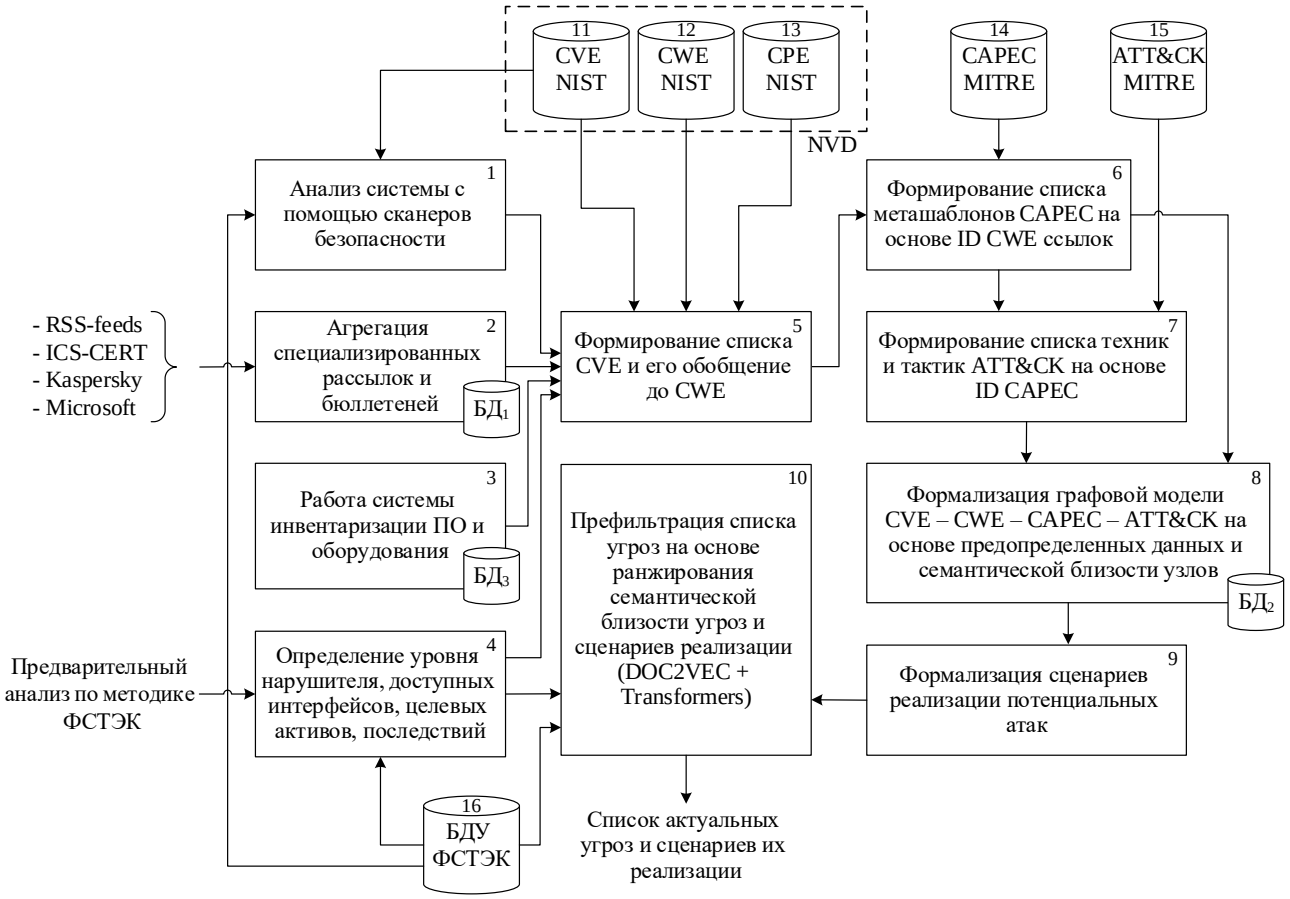


Рис. 11 Структура системы построения и анализа семантической модели текстовых описаний объектов зоны безопасности объекта КИИ.

Результирующая НСКК позволяет оценить риски ИБ при реализации воздействия нарушителя на инфраструктуру. Наиболее детализированный уровень НСКК отражает ряд действий нарушителя на каждом этапе реализации угрозы, что позволяет получить детализированную оценку риска ИБ для целевых объектов информационной инфраструктуры.

Метод и алгоритмы комплексной оценки рисков ИБ объектов КИИ

В [6] рассмотрен пример решения задачи оценки риска ИБ от реализации вирусной атаки с помощью нечетких продукционных когнитивных карт (НПКК) (рисунок 12).

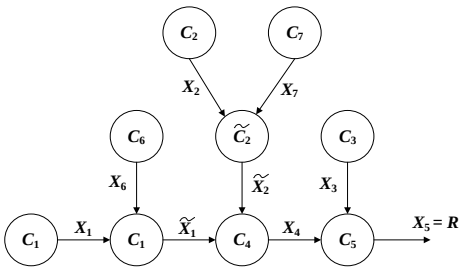


Рис. 12 Схема НПКК для оценки риска ИБ с учетом контрмер: C_1, C_2, C_3 – угроза, уязвимость и информационный ресурс; C_4 и C_5 – реализация угрозы и риск (потенциальный ущерб); C_6 и C_7 – ресурсы, выделяемые на парирование (блокирование) угрозы и устранение уязвимости; $\widetilde{C_1}$ и $\widetilde{C_2}$ – модифицированные (скомпенсированные за счет принятия контрмер) угроза и уязвимость.

Рассмотрены особенности применения НСКК для оценки рисков ИБ от нарушения конфиденциальности и целостности информации, вызванных воздействием на информационные активы угроз типа «Несанкционированный доступ» и «Вредоносное программное воздействие/вирусы» (рисунок 13).

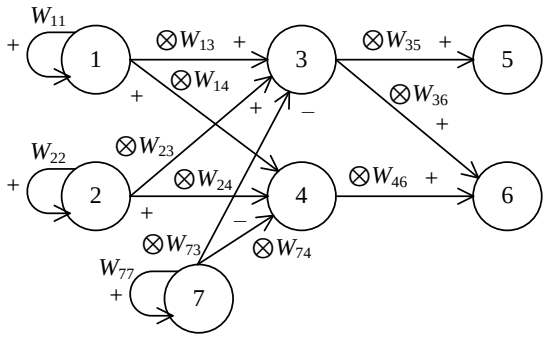


Рис. 13 Нечеткая серая когнитивная карта: *1* – концепт C_1, представляющий собой угрозу, связанную с попыткой несанкционированного доступа (НСД) к информации; *2* – концепт C_2, представляющий угрозу, связанную с вредоносным программным воздействием (вирусными атаками); *3* – концепт C_3, характеризующий целевой объект угрозы – базу данных (БД), размещенную на сервере; *4* – концепт C_4, характеризующий электронный документооборот (ЭДО) организации; *5* – концепт C_5, характеризующий потенциальный ущерб, вызванный нарушением конфиденциальности информации; *6* – концепт C_6, характеризующий потенциальный ущерб вследствие нарушения целостности информации при воздействии заданной угрозы.

Для оценки рисков ИБ в зоне безопасности объекта КИИ путем проведения сценарного моделирования предложено построение укрупненной НСКК с последующей ее декомпозицией на ряд вложенных НКК следующих уровней детализации. При построении вложенных НКК реализовано последовательное раскрытие неопределенностей – каждый последующий слой содержит более детальную (локальную) информацию о внутренней структуре базовых концептов исходной НКК (см. рисунок 13).

Предлагается методика анализа рисков ИБ с использованием построения вложенных нечетких когнитивных карт [18] на примере задачи обеспечения целостности телеметрической информации (ТМИ) в промышленной автоматизированной информационной системе (АИС) сбора, хранения и обработки информации о состоянии авиационных бортовых систем. В составе АИС выделены зоны безопасности, объединяемые по принципу единства выполняемых функций и требований к безопасности их реализации, связанные каналами телекоммуникаций (трактами).

В [10] рассмотрена задача анализа рисков ИБ, связанных с обеспечением целостности ТМИ АИС, с учетом воздействия на систему внешних и внутренних угроз, с помощью НСКК. Укрупненная НСКК для оценки рисков ИБ АИС, выступающая в данном случае как когнитивная модель АИС начального приближения, представлена на рисунке 14.

В [16] предложен сценарный подход к моделированию сложных многошаговых целенаправленных кибератак с использованием базы меташаблонов атак CAPEC и БДУ ФСТЭК России с формализацией в виде иерархической НКК для возможности анализа с требуемым уровнем детализации и количественной оценки рисков ИБ (рисунки 15 и 16).

Исходными данными для конструирования вектора атаки на основе меташаблонов являются результаты работы сканеров уязвимостей и базы данных угроз и уязвимостей, а также потенциальных слабостей программного и аппаратного обеспечения. Набор показателей системы оценки уязвимостей CVSS и базы CVE и CWE позволяют формально описать уязвимость и сценарий ее эксплуатации, а также автоматизировать процесс построения цепочки возможных переходов внутри меташаблона. Рассмотрен алгоритм построения укрупненной НКК для сформированного вектора атаки.

В [22] предложены рекомендации по повышению интерпретируемости результатов моделирования рисков ИБ, полученных с НКК.

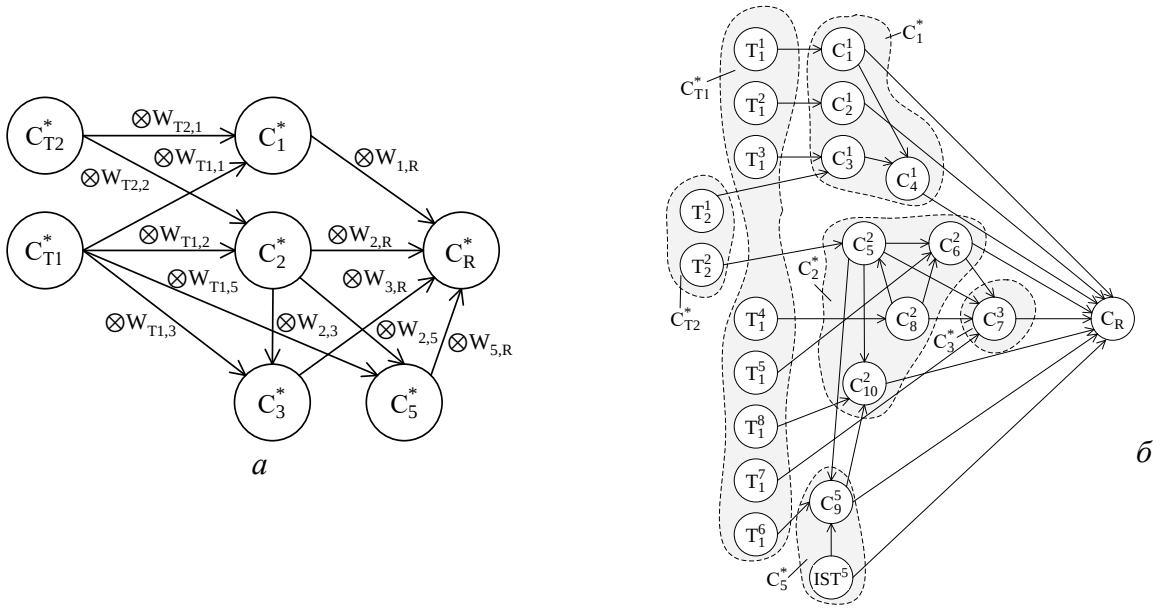


Рис. 14 Укрупненная (исходная) НСКК для оценки рисков ИБ (*а*) и первый уровень декомпозиции НСКК для оценки рисков ИБ АИС (*б*). Верхний индекс (маркер «*») обозначает принадлежность концепта C_p^* к укрупненной НСКК, нижний индекс (p) обозначает номер концепта текущего уровня.

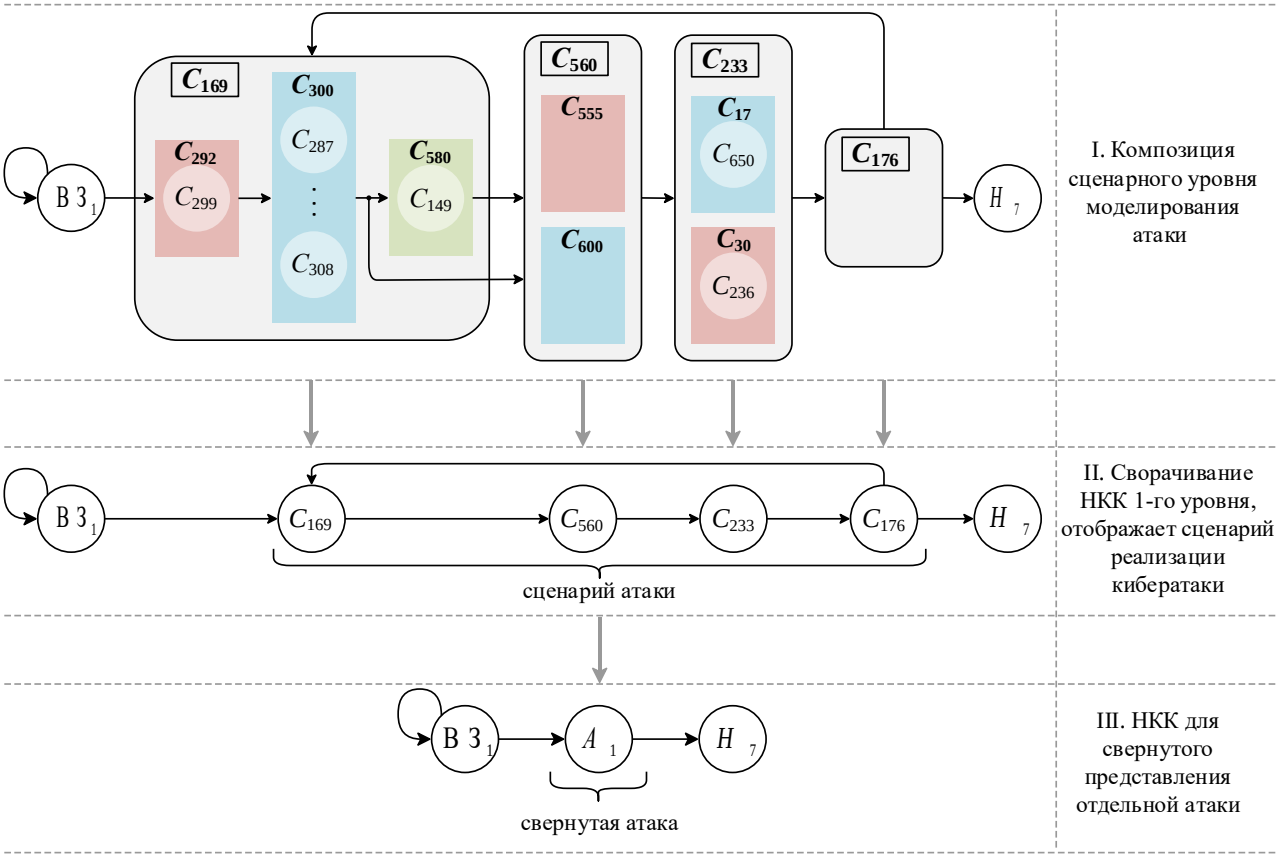


Рис. 15 Этапы построения укрупненной НКК для формирования графа атак.

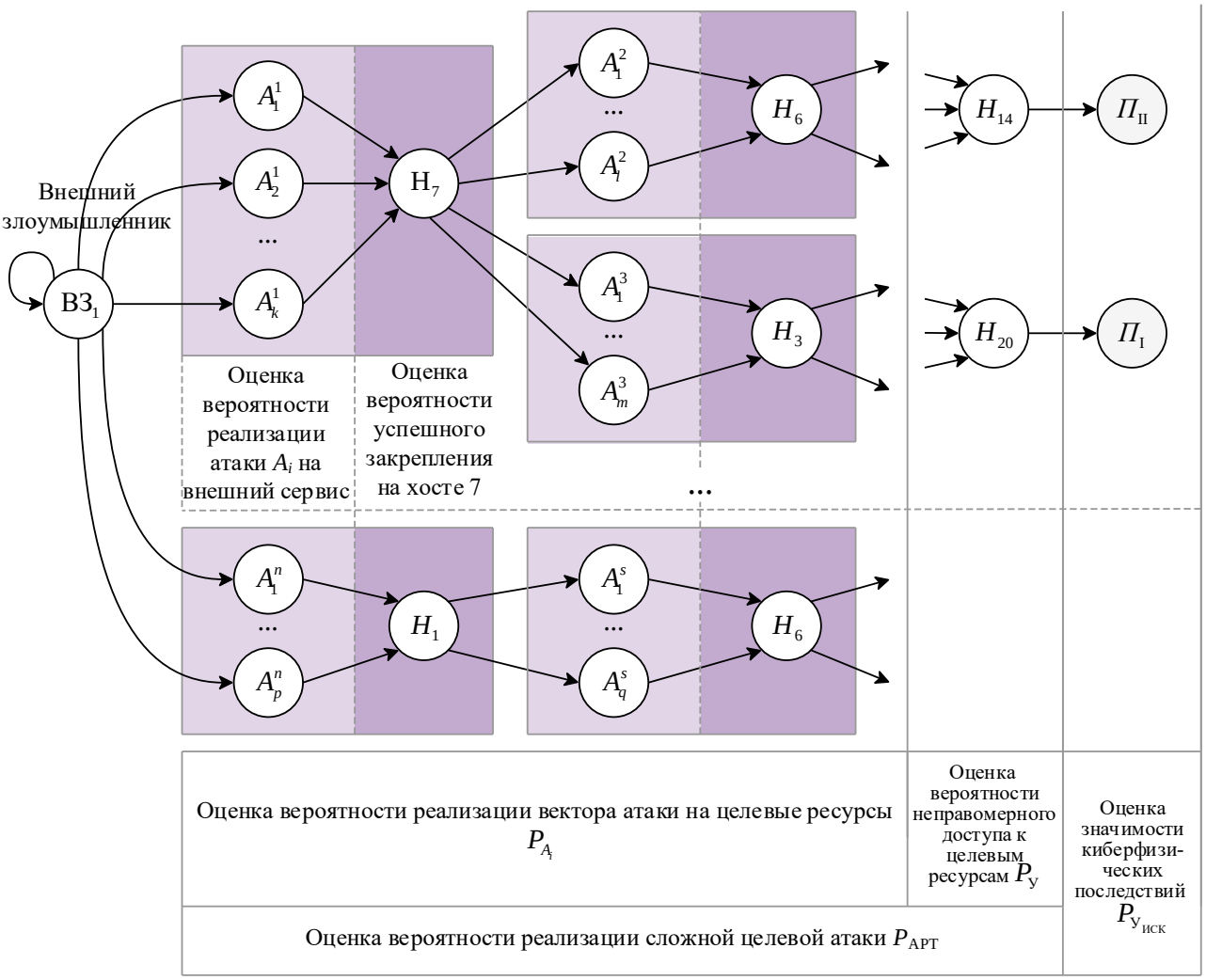


Рис. 16 НКК для моделирования набора возможных атак на выделенные целевые концепты.

Метод и алгоритм оценки риска ИБ

В [14, 44, 45] разработаны метод и алгоритмы оценки риска ИБ на основе обнаружения и анализа аномалий в накапливаемых данных мониторинга ИБ объекта КИИ с использованием технологий анализа временных рядов и методов машинного обучения. Переход от статической эталонной модели объекта КИИ и априорных оценок при анализе и оценке рисков ИБ к адаптивной модели объекта с уточнением вероятности реализации угроз, эксплуатации уязвимостей и итоговых оценок риска ИБ основан на применении методов мониторинга ИБ (наблюдение за объектом защиты, системой защиты и взаимодействием объекта с внешней средой).

В [46, 47] разработана структура системы мониторинга целостности ТМИ, основанная на обнаружении вызванных воздействием возможного злоумышленника аномалий в многомерных временных рядах, полученных с помощью модели сложного технического изделия и принимаемых с бортовых систем летательного аппарата (ЛА) (рисунок 17). Выходом системы мониторинга является оценка условной вероятности событий нарушения целостности данных. База нечетких продукционных правил применяется для объяснения принимаемого решения о типе согласования при необходимости проведения процедуры расследования инцидентов нарушения целостности ТМИ.

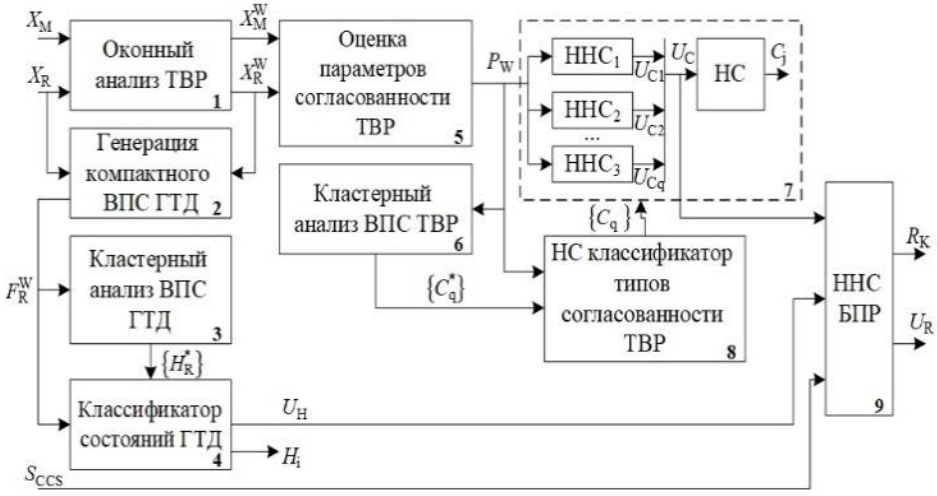


Рис. 17 Структурная схема системы анализа согласованности параметров ГТД, получаемых с модели и с борта ЛА: X_M – параметры состояния ГТД, полученные на основе модели; X_R – параметры состояния ГТД, полученные с борта ЛА; F_R^W – компактный вектор признаков состояния ГТД; R_K – результат мониторинга: «обрыв сигнала», «нормальная работа», «нарушение целостности»; U_R – вектор оценок вероятностей принадлежности текущего вектора параметров состояния одному из состояний мониторинга; ВПС – вектор признаков согласованности; ННС – нейронечеткий классификатор; БПР – блок принятия решений.

В [23] предложен способ мониторинга целостности данных о состоянии мобильного объекта (МО), основанный на сравнении ТВР, полученных от эксплуатируемого МО, и модели МО, установленной на предприятии-изготовителе. Для сравнения вычисляются следующие метрики близости: коэффициент детерминации, средний процент отклонения и евклидово расстояние, кроме того, принимается сигнал системы контроля исправности МО и идентифицируется режим работы МО (установившийся и переходный). Далее, в соответствии с выработанными правилами нечеткой логики, принимается решение о наличии или отсутствии атаки злоумышленника на принятые данные, их целостности. На рисунке 18 представлена структурная схема системы мониторинга целостности данных. По результатам экспериментов, оценка вероятности успешного распознавания атаки с помощью системы мониторинга целостности данных, основанного на правилах нечеткой логики, составила 0,85, а на основе нейронечеткого модуля – 0,98.

Алгоритм мониторинга целостности данных:

1. Выделяется набор параметров МО для анализа рассогласований данных, полученных с модели, и данных, полученных с МО.

2. Выделяется скользящее окно для анализа многомерных векторов $X, Y, YM, XM\, X_M^W, X_R^W$ – наборы ТВР, сгенерированные моделью и полученные с МО, в одном временном окне.

3. Строится многомерный временной ряд (ВР) P^W – параметры согласованности ТВР для каждого из окон анализа WS.

4. Определяется режим работы МО U_H в выделенном временном окне.

5. Выполняется расчет параметров согласованности ТВР, полученных с борта МО, и ТВР, генерируемых моделью.

6. По параметрам рассогласования на основе типа динамики МО и сигнала системы контроля принимается решение о целостности данных, полученных с МО.

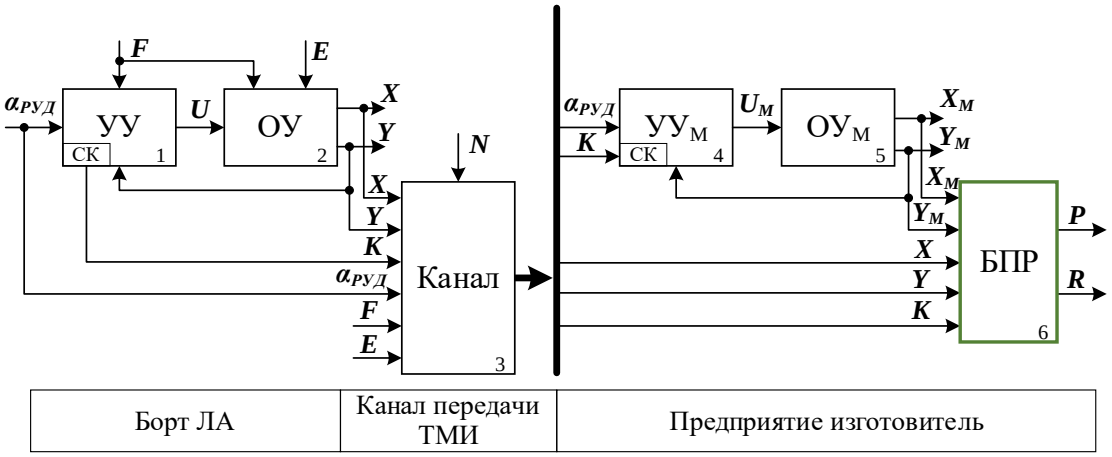


Рис. 18 Схема реализации системы мониторинга целостности данных, получаемых с бортовых систем мобильного объекта.

В [48–50] разработаны система обнаружения сетевых атак в гетерогенной сети промышленного объекта и алгоритм интеллектуального анализа сетевого трафика. С целью оценки их количественных и качественных характеристик использовались общедоступные размеченные по типам атак и режимам работы базы данных сетевого трафика (NSL-KDD, CICIDS-2017, UNSW-NB15, сети промышленного Интернета вещей – WUSTL-IIOT-2018; беспроводные промышленные сенсорные сети – WSN-DS-2016) и полусинтетические наборы, собранные с использованием полунатурного стенда, моделирующего взаимодействие промышленной сети и корпоративного сегмента. Особенностью указанных наборов данных является акцент на использование промышленных протоколов, таких как Modbus.

Структурная схема системы обнаружения сетевых атак в гетерогенной сети промышленного объекта на основе интеллектуального анализа данных и обобщенный алгоритм интеллектуального анализа параметров сетевого трафика в задаче обнаружения аномалий и вредоносной сетевой активности представлены на рисунке 19.

В составе подсистемы автоматического профилирования (рисунок 20) предложена обобщенная схема модуля видеоаналитики, позволяющего:

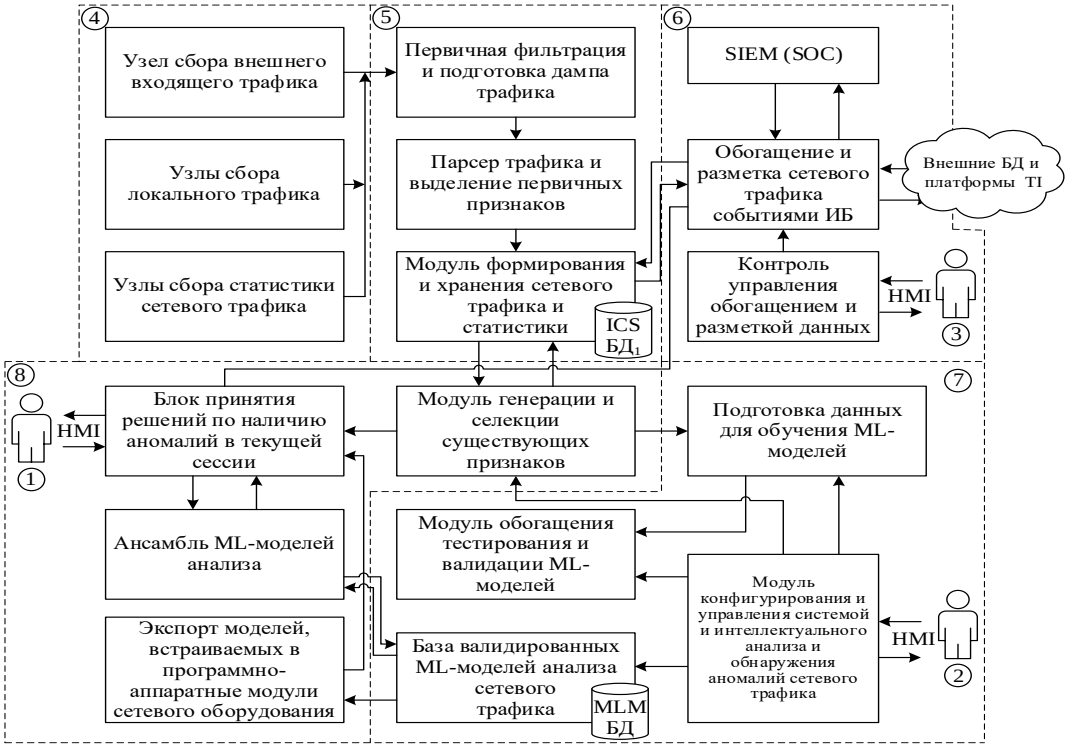
– анализировать, оценить степень уверенности композиции классификаторов в типе распознаваемого образа (аутентификация на основе изображения лица), динамике движений субъекта (распознавание типа движений, жестов), типе психоэмоционального состояния оператора (корректность классификации паттернов составила 97 %);

– выполнять функции нейросетевой системы идентификации и аутентификации пользователя.

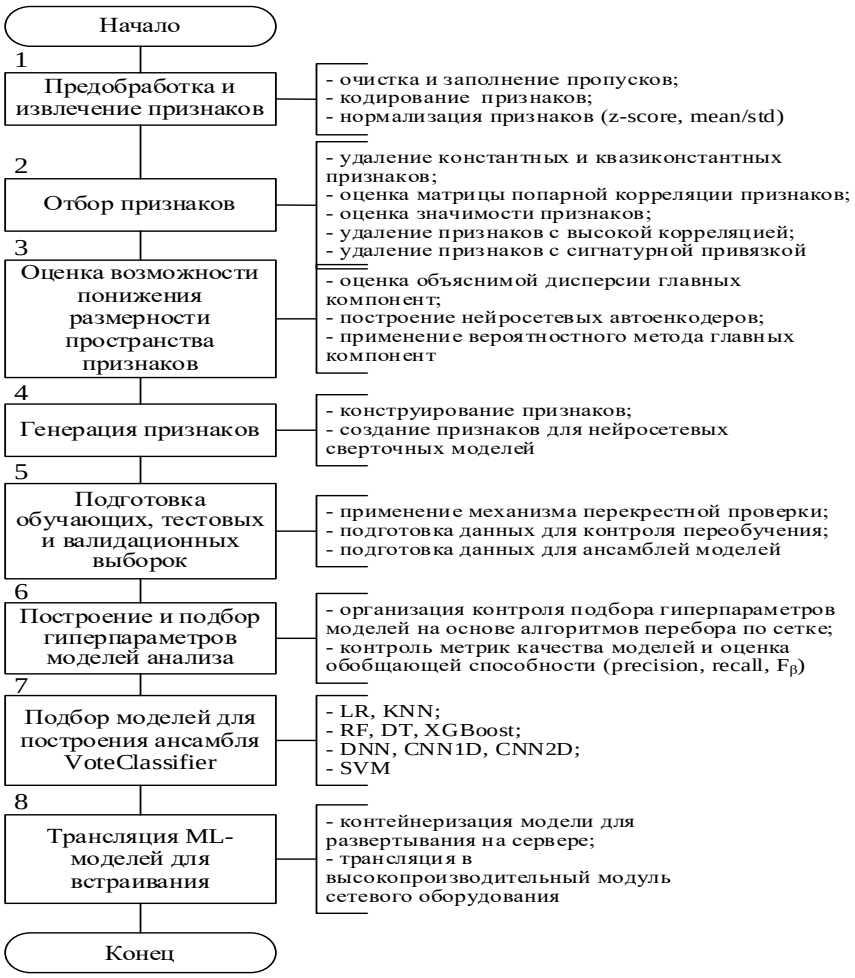
В функции подсистемы автоматического профилирования также входит анализ информационного почерка пользователя (динамический профиль пользователя на основе анализа клавиатурного почерка), позволяющего выполнять процедуру непрерывной скрытой идентификации и аутентификации (корректность классификации пользователя составила 98 %).

Прикладные задачи комплексной оценки рисков ИБ

В [1] разработана архитектура ИСППР по оценке рисков ИБ объектов КИИ, включающая в себя следующие базовые модули: подсистема анализа угроз и уязвимостей объекта КИИ на основе технологий семантического анализа их текстовых описаний; подсистема оценки степени опасности уязвимостей на основе прогнозирования набора метрик с помощью анализа текстового описания; подсистема построения и анализа семантической модели текстовых описаний, характеризующих аспекты безопасности программного и аппаратного обеспечения зоны безопасности объекта КИИ; подсистема обнаружения сетевых атак в гетерогенной сети объекта КИИ; подсистема автоматического профилирования.



а



б

Рис. 19 Структурная схема системы обнаружения сетевых атак на основе интеллектуального анализа данных и обобщенный алгоритм интеллектуального анализа сетевого трафика в задаче обнаружения аномалий и вредоносной сетевой активности.

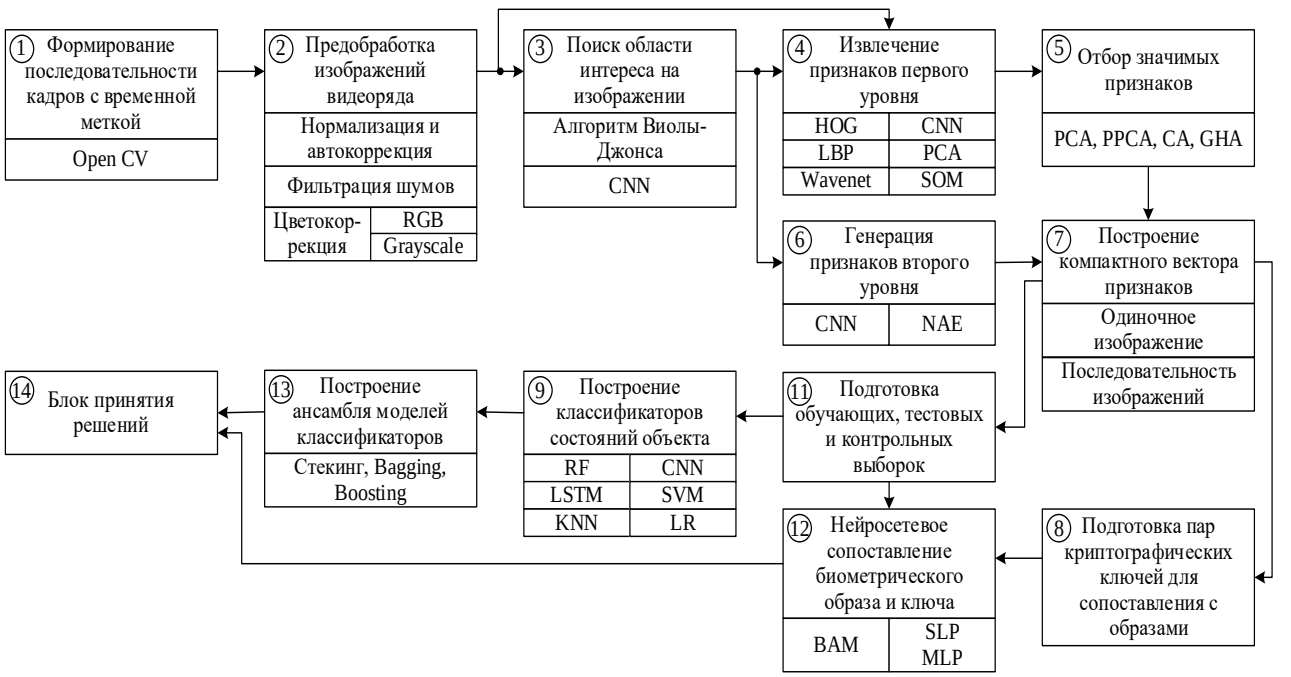


Рис. 20 Структура системы автоматического профилирования действий пользователя.

Особенностью данной ИСППР является возможность автоматизации основных этапов комплексной оценки рисков ИБ объектов КИИ, что позволяет отслеживать эволюцию объекта защиты и выполнять уточнение оценок вероятностей реализации угроз и эксплуатации уязвимостей, а также реализацию опережающей стратегии защиты (проактивная защита).

В качестве объекта КИИ рассмотрена АИС сбора, хранения и обработки ТМИ предприятия-изготовителя изделий авиационной техники [28]. Для автоматизации предложенной процедуры комплексной оценки рисков ИБ разработано прикладное алгоритмическое и программное обеспечение. Применение предложенного способа мониторинга целостности данных, получаемых с бортовых систем мобильного объекта, позволило снизить оценку риска ИБ для рассматриваемой системы на 45 %.

Предложено решение задачи оценки рисков ИБ промышленной сети АСУ ТП нефтедобывающего предприятия с использованием технологий когнитивного моделирования на основе классических, серых, интуиционистских НКК и их ансамбля, позволяющего учесть неопределенность мнений экспертов в оценке риска ИБ. Полученные оценки рисков ИБ после оптимизации распределения ресурсов, выделенных на контрмеры, уменьшились как в отношении разброса, так и в отношении центрального значения оценок на 70–80 %, снизилась оценка стоимости эксплуатации контрмер.

В процессе решения поставленной практической задачи противодействия кибермошенничеству (создания антифрод-системы) предложены алгоритм сбора, обработки данных, характеризующих пользовательское окружение конечной системы [21, 28, 31, 41], а также алгоритм анализа изменения паттернов динамических биометрических признаков пользователя в случае удаленного управления пользовательским сеансом. В качестве объекта воздействия угрозы (фрода) в данном случае выступает ИС, в которой хранится и обрабатывается информация, представляющая интерес для злоумышленника. Предложена гетерогенная модель обнаружения удаленного управления пользовательским сеансом на основе анализа цифрового отпечатка пользователя (точность 93 %).

В [51] проведен анализ угроз нарушения ИБ и соответствующих им мер противодействия по уровням архитектуры программно-определяемых сетей объектов КИИ. Разработаны и реализованы инструменты (алгоритмическое и программное обеспечение, архитектура системы взаимодействия) защиты управляющего трафика программно-определяемых сетей на основе

традиционных моделей машинного обучения и гетерогенных нейросетевых моделей (F_1-мера достигает 96 %) с возможностью программно-аппаратной реализации.

С целью осуществления мониторинга и обмена данными об инцидентах ИБ в финансовой сфере (в составе платформы IRP/SOAR) разработана структурная схема системы мониторинга банковских транзакций в составе антифрод-системы [52], которая включает модуль интеллектуального анализа текстовых меток операций. Внедрение модуля позволяет делать выводы о принадлежности транзитной операции к одному из предложенных классов, строить динамический профиль пользователя и повысить обоснованность рекомендаций системы мониторинга (точность классификации операций составила 81 %).

Разработан проблемно-ориентированный программный комплекс «Полигон» [53], предназначенный для тестирования и отладки методов, моделей и алгоритмов когнитивного моделирования и интеллектуального анализа слабоструктурированных данных при построении базы знаний ИСППР, реализованный на масштабируемой (открытой) инструментальной платформе (в том числе на кластерной) с возможностью сопряжения / встраивания в существующие системы корреляции событий ИБ и ситуационные операционные центры.

Заключение

Таким образом, разработаны научно обоснованные технические и технологические решения, направленные на решение проблемы разработки моделей и методов комплексной оценки рисков ИБ объектов КИИ на основе методов и технологий интеллектуального анализа данных, имеющей важное хозяйственное значение. Основные выводы и результаты работы можно сформулировать следующим образом:

1. Предложена концепция комплексной оценки рисков ИБ объектов КИИ, основанная на интеграции технологий нечеткого когнитивного моделирования и методов машинного обучения, отличающаяся применением комплекса проблемно-ориентированных моделей, методов и алгоритмов комплексной оценки рисков ИБ объектов КИИ, что позволяет повысить оперативность и снизить эффект неопределенности от влияния субъективных факторов.

2. Разработан комплекс проблемно-ориентированных моделей параметризации угроз и уязвимостей объектов КИИ, основанных на использовании технологий интеллектуального анализа данных и обнаружения аномалий в накапливаемых данных мониторинга их состояния, отличающийся применением ансамбля гетерогенных моделей машинного обучения при оценке опасности уязвимостей и построении детекторов аномалий и эффективным использованием дополнительной информации из открытых баз знаний с помощью технологий анализа текстовых описаний, что позволяет снизить трудоемкость и автоматизировать низкоуровневое моделирование сценариев эксплуатации уязвимостей и реализации угроз, а также обеспечивает видимость и контекст потенциальной атаки.

3. Разработаны метод, алгоритмы и методика качественной оценки уровня рисков ИБ объектов КИИ, основанные на использовании технологий семантического анализа текстовых описаний угроз и уязвимостей, отличающиеся подходом к формализации слабоструктурированных текстовых описаний с помощью гетерогенных нейросетевых моделей вложений в виде графовой семантической модели, что позволяет обеспечить выявление потенциальных угроз, уязвимостей и сценариев реализации атак с возможностью их ранжирования по приоритетам, а также автоматизировать основные этапы процедуры оценки рисков.

4. Разработаны метод, алгоритмы и методика количественной оценки рисков ИБ объектов КИИ, основанные на построении иерархии вложенных когнитивных карт, соответствующих структурно-функциональной организации объекта КИИ, отличающиеся построением и декомпозицией укрупненной нечеткой когнитивной карты, сценарным моделированием сложных многошаговых целенаправленных кибератак с использованием базы меташаблонов атак с дальнейшей формализацией в виде иерархической НКК, что позволяет получить количе-

ственную оценку рисков ИБ объектов КИИ с учетом совокупности объективных и субъективных факторов неопределенности, а также автоматизировать сценарное моделирование сложных многошаговых атак с использованием базы меташаблонов.

5. Разработаны метод и алгоритмы оценки рисков ИБ объектов КИИ на основе обнаружения аномалий временных рядов накапливаемых параметров, характеризующих состояние этих объектов, сетевого трафика промышленных сетей и поведения пользователей конечных систем, основанные на применении методов интеллектуального анализа многомерных временных рядов, что позволяет повысить достоверность и оперативность поиска скрытых зависимостей в накапливаемых данных и повысить достоверность результатов оценивания рисков ИБ за счет уточнения априорных оценок вероятностей реализации угроз и эксплуатации уязвимостей.

6. Разработана архитектура ИСППР по оценке рисков ИБ объектов КИИ, интегрирующая предложенные в работе технические решения. Проведенные исследования с использованием данной ИСППР показывают, что:

– применение предложенного способа мониторинга целостности телеметрических данных, получаемых с бортовых систем мобильного объекта, позволило снизить оценку риска ИБ для рассматриваемой системы на 45%; оценка вероятности успешного распознавания атаки с помощью системы мониторинга целостности данных, основанного на правилах нечеткой логики, составила 0,85, а на основе нейронечеткого модуля – 0,98;

– предложенные алгоритмы обнаружения аномалий в данных мониторинга состояния АСУ ТП нефтедобычи позволяют корректно классифицировать до 78–95 % состояний, в том числе вызванных воздействием злоумышленника;

– предложенные решения по цифровому профилированию и анализу совокупности отпечатков (fingerprints) пользовательских окружений и динамических пользовательских профилей в задаче противодействия кибермошенничеству (создания антифрод-системы) обеспечивают повышение точности определения удаленного управления на 17 % и повышение точности классификации мошеннических операций на 23 %;

– предложенные решения в задачах обнаружения аномалий сетевого трафика в гетерогенных промышленных сетях позволяют добиться оценки F_1-меры на уровне 96 %.

Дальнейшее развитие этого исследования планируется в двух направлениях:

– исследование технологий ИАД текстовых описаний угроз и уязвимостей на основе моделей трансформеров, что позволит использовать мультиязычные базы знаний для сопоставления угроз, уязвимостей и сценариев их эксплуатации и повысит достоверность оценок рисков ИБ;

– исследование методов и алгоритмов моделирования сложных технических объектов с применением специализированных глубоких нейронных сетей с целью повысить достоверность результатов оценивания рисков ИБ за счет уточнения априорных оценок вероятностей реализации угроз и эксплуатации уязвимостей.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

1. Васильев В. И., Вульфин А. М., Гвоздев В. Е., Картак В. М., Атарская Е. А. Обеспечение информационной безопасности киберфизических объектов на основе прогнозирования и обнаружения аномалий их состояния // Системы управления, связи и безопасности. 2021. № 6. С. 90–119. DOI: 10.24412/2410-9916-2021-6-90-119. [[V. I. Vasilyev, A.M. Vulfin, V. E. Gvozdev, V. M. Kartak and E. A. Atarskaya, Ensuring information security of cyber-physical objects based on predicting and detecting anomalies in their state (in Russian) // Systems of Control, Communication and Security, vol. 6, pp. 90-119, 2021.]]

2. Актуальные киберугрозы: II квартал 2023 года [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q2/ (дата обращения: 29.08.2023). [[Current Cyber Threats: Q2 2023 [Online], (in Russian). URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q2/ (2023, Aug. 29)]]

3. Первое полугодие 2023 года – краткий обзор основных инцидентов промышленной кибербезопасности [Электронный ресурс]. URL: https://ics-cert.kaspersky.ru/publications/reports/2023/10/05/h1-2023-a-brief-overview-of-main-incidents-in-industrial-cybersecurity/ (дата обращения: 05.10.2023). [[H1 2023 – A Brief Overview of Main Incidents in Industrial Cybersecurity [Online], (in Russian). URL: https://ics-cert.kaspersky.ru/publications/reports/2023/10/05/h1-2023-a-brief-overview-of-main-incidents-in-industrial-cybersecurity/ (2023, Oct. 05)]]

4. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 г. [Электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kii/285-zakony/1610-federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz (дата обращения: 20.09.2023). [[Federal Law No. 187-FZ “On the security of critical information infrastructure of the Russian Federation” dated July 26, 2017 [Online], (in Russian). URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kii/285-zakony/1610-federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz (2023, Sep. 20)]]

5. Распоряжение № 1632-р «Программа «Цифровая экономика Российской Федерации»» от 28.07.2017 г. [Электронный ресурс]. URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения: 20.08.2023). [[Order No. 1632-r “Program “Digital Economy of the Russian Federation” dated July 28, 2017 [Online], (in Russian). URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (2023, Aug. 20)]]

6. Васильев В. И., Вульфин А. М., Кудрявцева Р. Т. Анализ и управление рисками информационной безопасности с использованием технологии нечеткого моделирования // Доклады ТУСУРа. 2017. Т. 20. № 4. С. 61–66. [[V. I. Vasilyev, A.M. Vulfin and R. T. Kudryavtseva. Analysis and management of information security risks using cognitive modeling technology (in Russian) // Proceedings of TUSUR University, vol. 20, no. 4, pp. 61-66, 2017.]]

7. Васильев В. И., Гузаиров М. Б., Вульфин А. М. Оценка рисков информационной безопасности с использованием нечетких продукционных когнитивных карт // Информационные технологии. 2018. Т. 24. № 4. С. 266–273. [[V. I. Vasilyev, M. B. Guzairov, and A. M. Vulfin. Evaluation of information security risks with use of rule-based fuzzy cognitive maps (in Russian) // Information Technology, vol. 24, no. 4, pp. 266-273, 2018.]]

8. Гузаиров М. Б., Вульфин А. М., Картак В. М., Кириллова А. Д., Миронов К. В. Сравнительный анализ алгоритмов когнитивного моделирования при оценке рисков информационной безопасности // Труды ИСА РАН. 2019. Т. 69. № 4. С. 62–69. [[M. B. Guzairov, A.M. Vulfin, V. M. Kartak, A. D. Kirillova and K. V. Mironov. Comparative analysis of algorithms for cognitive modeling in assessing information security risks (in Russian) // Proceedings of the ISA RAS, vol. 69, no. 4, pp. 62-69, 2019.]]

9. Васильев В. И., Вульфин А. М., Картак В. М., Кириллова А. Д., Миронов К. В. Система обнаружения атак в беспроводных сенсорных сетях промышленного интернета вещей // Труды ИСА РАН. 2019. Т. 69. № 4. С. 70–78. [[V. I. Vasilyev, A. M. Vulfin, V. M. Kartak, A. D. Kirillova and K. V. Mironov. System of attacks detection in wireless sensor networks of Industrial Internet of Things (in Russian) // Proceedings of the ISA RAS, vol. 69, no. 4, pp. 70-78, 2019.]]

10. Vasilyev V. I., Vulfin A. M. and Chernyakhovskaya L. R. Cybersecurity risk analysis of industrial automation systems on the basis of cognitive modeling technology // Digital Forensic Science. IntechOpen, 2019. DOI: 10.5772/intechopen.78450.

11. Васильев В. И., Черняховская Л. Р., Вульфин А. М. Моделирование процессов управления инновационной деятельностью в регионе с применением нечетких когнитивных карт // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2020. № 3. С. 15–25. [[V. I. Vasilyev, L. R. Chernyakhovskaya, and A. M. Vulfin. Modeling of innovative activity management processes in the region with use of fuzzy cognitive maps (in Russian) // Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics, no. 3, pp. 15-25, 2020.]]

12. Васильев В. И., Вульфин А. М., Черняховская Л. Р. Анализ рисков инновационных проектов с использованием технологии многослойных нечетких когнитивных карт // Программная инженерия. 2020. Т. 11. № 3. С. 142–151. [[V. I. Vasilyev, A. M. Vulfin and L. R. Chernyakhovskaya. Risk analysis of innovative projects with use of multilayer fuzzy cognitive maps (in Russian) // Software Engineering, vol. 11, no. 3, pp. 142-151, 2020.]]

13. Васильев В. И., Вульфин А. М., Кириллова А. Д., Черняховская Л. Р. Об интерпретируемости нечетких когнитивных моделей на этапе оценки рисков инновационных проектов // Вестник УрФО. Безопасность в информационной сфере. 2019. № 4(34). С. 45–57. [[V. I. Vasilyev, A. M. Vulfin, A. D. Kirillova and L. R. Chernyakhovskaya. On the interpretability of fuzzy cognitive models at the stage of risks assessment for innovative projects (in Russian) // Vestnik UrFO. Security in the Information Sphere, vol. 4(34), pp. 45-57, 2019.]]

14. Вульфин А. М. Анализ защищенности веб-приложения для доступа к системе хранения критически важных данных [Электронный ресурс] // Моделирование, оптимизация и информационные технологии. 2021. № 9(4). С. 1–16. DOI: 10.26102/2310-6018/2021.35.4.038. URL: https://moitvivt.ru/ru/journal/pdf?id=1112 (дата обращения: 20.09.2023) [[A. M. Vulfin, “Security analysis of a web application for accessing the critical data storage system,” [Online], (in Russian) // Modeling, Optimization and Information Technology, no. 9(4), pp. 1-16, 2021. DOI: 10.26102/2310-6018/2021.35.4.038. URL: https://moitvivt.ru/ru/journal/pdf?id=1112 (2023, Sep. 20)]]

15. Васильев В. И., Вульфин А. М., Кучкарова Н. В. Автоматизация анализа уязвимостей программного обеспечения на основе технологии Text Mining // Вопросы кибербезопасности. 2020. № 4(38). С. 22–31. [[V. I. Vasilyev, A. M. Vulfin, and N. V. Kuchkarova. Automation of software vulnerabilities analysis on the basis of text mining technology (in Russian) // Cybersecurity Issues, vol. 4(38), pp. 22-31, 2020.]]

16. Васильев В. И., Кириллова А. Д., Вульфин А. М. Когнитивное моделирование вектора кибератак на основе меташаблонов CAPEC // Вопросы кибербезопасности. 2021. № 2(42). С. 2–16. [[V. I. Vasilyev, A. D. Kirillova and A. M. Vulfin. Cognitive modeling of the cyber attack vector based on CAPEC methods (in Russian) // Cybersecurity Issues, vol. 2(42), pp. 2-16, 2021.]]

17. Вульфин А.М. Система управления данными киберразведки [Электронный ресурс] // Моделирование, оптимизация и информационные технологии. 2021. № 9(1). С. 1–18. DOI: 10.26102/2310-6018/2021.32.1.020. URL: https://moitvivt.ru/ru/journal/pdf?id=925 [[A. M. Vulfin. Cyber threat intelligence data management system [Online], (in Russian) // Modeling, Optimization and Information Technology, no. 9(1), pp. 1-18, 2021. DOI: 10.26102/2310-6018/2021.32.1.020. URL: https://moitvivt.ru/ru/journal/pdf?id=925 (2023, Sep. 20)]]

18. Васильев В. И., Вульфин А. М., Кириллова А. Д., Кучкарова Н. В. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining // Системы управления, связи и безопасности. 2021. № 3.

С. 110–134. [[V. I. Vasilyev, A. M. Vulfin, A. D. Kirillova and N. V. Kuchkarova. Methodology for assessing current threats and vulnerabilities based on cognitive modeling technologies, and Text Mining (in Russian) // Systems of Control, Communication and Security, no. 3, pp. 110-134, 2021.]]

19. Васильев В. И., Вульфин А. М., Гузаиров М. Б., Картак В. М., Черняховская Л. Р. Оценка рисков кибербезопасности АСУ ТП промышленных объектов на основе вложенных нечетких когнитивных карт // Информационные технологии. 2020. Т. 26. № 4. С. 213–221. [[V. I. Vasilyev, A. M. Vulfin, M. B. Guzairov, V. M. Kartak and L. R. Chernyakhovskaya. Assessment of cybersecurity risks of automated process control systems of industrial facilities based on nested fuzzy cognitive maps (in Russian) // Information Technology, vol. 26, no. 4, pp. 213-221, 2020.]]

20. Вульфин А. М. Интеллектуальный анализ видеоданных в системе контроля соблюдения правил промышленной безопасности [Электронный ресурс] // Моделирование, оптимизация и информационные технологии. 2020. № 8(2). С. 1–16. DOI: 10.26102/2310-6018/2020.29.2.010. URL: https://moit.vivt.ru/wp-content/uploads/2020/05/Vulfin_2_20_1.pdf (дата обращения: 20.09.2023) [[A. M. Vulfin. Intelligent analysis of video data in system for monitoring compliance with industrial safety rules [Online], (in Russian) // Modeling, Optimization and Information Technology, no. 8(2), pp. 1-16, 2020. DOI: 10.26102/2310-6018/2020.29.2.010. URL: https://moit.vivt.ru/wp-content/uploads/2020/05/Vulfin_2_20_1.pdf (2023, Sep. 20)]]

21. Вульфин А. М. Интеллектуальный анализ данных пользовательского окружения в задаче обнаружения удаленного управления [Электронный ресурс] // Моделирование, оптимизация и информационные технологии. 2020. № 8(2). С. 1–19. DOI: 10.26102/2310-6018/2020.29.2.011. URL: https://moit.vivt.ru/wp-content/uploads/2020/05/Vulfin_2_20_2.pdf (дата обращения: 20.09.2023) [[A. M. Vulfin. Data mining the user's environment in the problem of remote control detection [Online], (in Russian) // Modeling, Optimization and Information Technology, no. 8(2), pp. 1-19, 2020. DOI: 10.26102/2310-6018/2020.29.2.011. URL: https://moit.vivt.ru/wp-content/uploads/2020/05/Vulfin_2_20_2.pdf (2023, Sep. 20)]]

22. Васильев В. И., Вульфин А. М., Герасимова И. Б., Картак В. М. Анализ рисков кибербезопасности с помощью нечетких когнитивных карт // Вопросы кибербезопасности. 2020. № 2(36). С. 11–21. [[V. I. Vasilyev, A. M. Vulfin, I. B. Gerasimova, and V. M. Kartak. Analysis of cybersecurity risk with use of fuzzy cognitive maps (in Russian) // Cybersecurity Issues, vol. 2(36), pp. 11-21, 2020.]]

23. Фрид А. И., Вульфин А. М., Берхольц В. В. Способ мониторинга целостности телеметрической информации о состоянии двигателя летательного аппарата // Безопасность информационных технологий. 2020. Т. 27. № 4. С. 65–76. [[A. I. Frid, A. M. Vulfin and V. V. Berkholts. The method of aviation gas turbine engine state information integrity monitoring (in Russian) // IT Security, vol. 27, no. 4, pp. 65-76, 2020.]]

24. Васильев В. И., Вульфин А. М., Гузаиров М. Б., Кириллова А. Д. Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт // Информационные технологии. 2018. Т. 24. № 10. С. 657–664. [[V. I. Vasilyev, A. M. Vulfin, M. B. Guzairov and A. D. Kirillova. Interval estimation of information risks with use of fuzzy grey cognitive maps (in Russian) // Information Technologies, vol. 24, no. 10, pp. 657-664, 2018.]]

25. Васильев В. И., Вульфин А. М., Кириллова А. Д., Никонов А. В. Система оценки метрик опасности уязвимостей на основе технологий семантического анализа данных // Вестник УрФО. Безопасность в информационной сфере. 2021. № 2(40). С. 31–43. [[V. I. Vasilyev, A. M. Vulfin, A. D. Kirillova and A. V. Nikonov. System for evaluating vulnerability severity metrics based on semantic data analysis technologies (in Russian) // Vestnik UrFO. Security in the Information Sphere, vol. 2(40), pp. 31-43, 2021.]]

26. Вульфин А. М., Фрид А. И. Нейросетевая модель анализа технологических временных рядов в рамках методологии Data Mining // Информационно-управляющие системы. 2011. № 5(54). С. 31–38. [[A. M. Vulfin and A. I. Frid. Neuralbase model analysis of technological time series within the scope of data mining strategy (in Russian) // Information and Control Systems, no. 5(54), pp. 31-38, 2011.]]

27. Vulfin A. M., Frid A. I. and Giniyatullin V. M. Neural-base model for detection and recognition of technological situations within the scope of data mining strategy // Optical Memory and Neural Networks (Information Optics). 2010. Vol. 19. No. 3. Pp. 207–212.

28. Guzairov M. B., Frid A. I., Vulfin A. M. and Berkholts V. V. Simulation modelling of the transmission system of the telemetric information on the status of the on-board aircraft status//4th International Conference on Information Technology and Nanotechnology: CEUR Workshop Proceedings, 2018. Pp. 105–111.

29. Arpishkin M. I., Vulfin A. M., Vasilyev V. I. and Nikonov A.V. Intelligent integrity monitoring system for technological process data // Journal of Physics: Conference Series. IOP Publishing. 2019. Vol. 1368. No. 5. Pp. 1–16.

30. Sapozhnikova M. U., Nikonov A. V., Vulfin A. M., Gayanova M. M., Mironov K. V. and Kurennov D. V. Anti-fraud system on the basis of Data Mining technologies //2017 IEEE International Symposium on Signal Processing and Information Technology. IEEE, 2017. Pp. 243–248.

31. Sapozhnikova M. U., Gayanova M. M., Vulfin A. M., Nikonov A. V. and Chuykov A. V. Distributed infrastructure for Big Data processing in the transaction monitoring systems//4th International Conference on Information Technology and Nanotechnology: CEUR Workshop Proceedings, 2018. Pp. 228–235.

32. Гаянова М. М., Вульфин А. М. Структурно-семантический анализ научных публикаций выделенной предметной области // Системная инженерия и информационные технологии. 2022. Т. 4. № 1(8). С. 37–43. [[M. M. Gayanova and A. M. Vulfin. Structural and semantic analysis of scientific publications in a selected subject area (in Russian) // Systems Engineering and Information Technologies, vol. 4, no. 1, pp. 37-43, 2022.]]

33. Жумажанова С. С., Сулавко А. Е., Ложников П. С. Распознавание психофизиологического состояния субъектов-операторов на основе анализа термографических изображений лица с применением сверточных нейронных сетей // Системная инженерия и информационные технологии. 2023. Т. 5. № 2(11). С. 41–55. [[S. S. Zhumazhanova, A. E. Sulavko and P. S. Lozhnikov. Recognition of the psychophysiological state of subject-operators based on the analysis of thermographic images of the face using convolutional neural networks (in Russian) // Systems Engineering and Information Technologies, vol. 5, no. 2(11), pp. 41-55, 2023.]]

34. Самотуга А. Е. Распознавание субъектов и их психофизиологических состояний на основе параметров подписи для защиты документооборота // Системная инженерия и информационные технологии. 2023. Т. 5. № 2(11). С. 56–65. [[A. E. Samotuga. Recognition of subjects and their psychophysiological states based on signature parameters to protect document management (in Russian) // Systems Engineering and Information Technologies, vol. 5, no. 2(11), pp. 56-65, 2023.]]

35. Startseva A. S., Vulfin A. M., Vasilyev V. I., Nikonov A. V. and Kirillova A. D. Analysis of financial payments text labels in the dynamic client profile construction // 2020 International Conference on Information Technology and Nanotechnology (ITNT). IEEE, 2020. Pp. 1–10.

36. Sivova A. A., Vulfin A. M., Mironov K. V. and Kirillova A. D. Hidden authentication of the user based on neural network analysis of the dynamic profile //Proceedings of the 8th International Conference on Applied Innovations in IT, 2020. Pp. 1–10.

37. Frid A. I., Vulfin A. M., Berholz V. V., Zakharov D. Yu. and Mironov K. V. Architecture of the security access system for information on the state of the automatic control systems of aircraft // Acta Polytechnica Hungarica. 2020. Vol. 17. No. 8. Pp. 151–164.

38. Hajrullin E. R., Vulfin A. M., Mironov K. V., Frid A. I., Guzairov M. B. and Kirillova A. D. Secure data exchange in the industrial internet of things network of the fuel and energy complex // Proceedings ICOECS 2020 International Conference on Electro-technical Complexes and Systems. IEEE, 2020. Pp. 353–358.

39. Vulfin A. M., Vasilyev V. I., Nikonov A. V. and Kirillova A. D. Neural network biometric cryptography system // Proceedings of the Information Technologies and Intelligent Decision Making Systems (ITIDMS2021). CEUR, 2021. Vol. 2843.

40. Vulfin A. M., Vasilyev V. I., Kirillova A. D. and Nikonov A. V. Cognitive security modeling of biometric system of neural network cryptography //Proceedings of the Information Technologies and Intelligent Decision Making Systems (ITIDMS2021). CEUR, 2021. Vol. 2843.

41. Sapozhnikova M. U., Nikonov A. V. and Vulfin A. M. Intrusion detection system based on data mining technics for industrial networks //International Conference on Industrial Engineering, Applications and Manufacturing, (ICIEAM). IEEE, 2018. Pp. 1–5.

42. Чуйков А. В., Вульфин А. М., Васильев В. И. Нейросетевая система преобразования биометрических признаков пользователя в криптографический ключ // Доклады ТУСУРа. 2018. Т. 21. № 3. С. 35–41. [[A. V. Chuikov, A.M. Vulfin and V. I. Vasilyev. Neural network system for converting the user biometric characteristics into a cryptographic key (in Russian) // Proceedings of TUSUR University, vol. 21, no. 3, pp. 35-41, 2018.]]

43. Методы и модели поддержки принятия решений при управлении инновационными проектами в производственно-экономических системах / Под общей ред. Л. Р. Черняховской (Глава 3: Анализ и управление рисками инновационных проектов и промышленных объектов с помощью технологий когнитивного моделирования. С. 118–157). М.: Издательский Дом «Академия Естествознания», 2020. [[Methods and Models for Decision Support in Managing Innovative Projects in Production and Economic Systems / Ed. Chernyakhovskaya L. R. (Chapter 3: “Analysis and risk management of innovative projects and industrial facilities using cognitive modeling technologies”. Pp. 118–157). (in Russian). Moscow: Publishing House "Academy of Natural Sciences", 2020.]]

44. Гузаиров М. Б., Вульфин А. М., Фрид А. И., Берхольц В. В. Защищенный доступ к базе данных о состоянии систем автоматического управления (САУ) авиационными ГТД через веб-приложение // Информация и безопасность. 2017. Т. 20. № 3. С. 410–413. [[M. B. Guzairov, A. M. Vulfin, A. I. Frid, V. V. Berkholts Secure access to the database on the state of automatic control systems (ACS) of aviation gas turbine engines via a web application (in Russian) // Information and Security, vol. 20, no. 3, pp. 410-413, 2017.]]

45. Berkholts V. V., Vulfin A. M. and Frid A. I. Telemetry data integrity monitoring system// IOP Conf. Series: Materials Science and Engineering. 2021. Vol. 1069. Pp. 012003.

46. Frid A. I., Vulfin A. M. and Berkholts V. V. Architecture of modular system for assessing security of telemetry information transmission system //International Conference on Industrial Engineering, Applications and Manufacturing, (ICIEAM). IEEE, 2018. Pp. 1–6.

47. Guzairov M. B., Frid A. I., Vulfin A. M. and Berkholts V. V. The concept of integrity of telemetric information about the state of an aircraft power plant monitoring //2019 International Conference on Electrotechnical Complexes and Systems (ICOECS). IEEE, 2019. Pp. 1–6.

48. Вульфин А. М. Обнаружение сетевых атак в гетерогенной промышленной сети на основе технологий машинного обучения // Программная инженерия. 2022. Т. 13. № 2. С. 68–80. DOI: 10.17587/prin.13.68-80 [[A. M. Vulfin. Detection of network attacks in a heterogeneous industrial network based on machine learning technologies (in Russian) // Software Engineering, vol. 13, no. 2, pp. 68-80, 2022.]]

49. Vulfin A. M., Vasilyev V. I., Kuharev S. N., Homutov E. V. and Kirillova A. D. Algorithms for detecting network attacks in an enterprise industrial network based on data mining algorithms // Journal of Physics: Conference Series. IOP Publishing. 2021. Vol. 2001. Pp. 012004.

50. Махмутов А. Р., Вульфин А. М., Миронов К. В. Исследование возможностей автономной работы конечных устройств интернета вещей // Системная инженерия и информационные технологии. 2023. Т. 5. № 1(10). С. 41–47. [[A. R. Makhmutov, A. M. Vulfin, K. V. Mironov. Research of the autonomous operation time of IoT end devices (in Russian) // Systems Engineering and Information Technologies, vol. 5, no. 1(10), pp. 41-47, 2023.]]

51. Makhmutov A. R., Trishin S. V., Mironov K. V. and Vulfin A. M. Software-hardware complex for modeling secure IIoT distributed ledger// IOP Conf. Series: Materials Science and Engineering. 2021. Vol. 1069. Pp. 012018.

52. Gurin M. A., Vulfin A. M., Vasilyev V. I. and Nikonov A. V. Intrusion detection system on the basis of data mining algorithms in the industrial network //5th International Conference on Information Technology and Nanotechnology: CEUR Workshop Proceedings, 2019. Pp. 553–565.

53. Vulfin A. M., Vasilyev V. I., Gvozdev V. E., Mironov K. V. and Churkin O. E. Network traffic analysis based on machine learning methods // Journal of Physics: Conference Series. 2021. Vol. 2001. Pp. 012017.

Поступила в редакцию 7 сентября 2023 г.

МЕТАДАННЫЕ / METADATA

Title: Models and methods for comprehensive assessment of security risks of critical information infrastructure objects based on intelligent data analysis.

Abstract: The article presents an overview of the results of a study of a multi-level distributed information management system – an object of critical information infrastructure (CII), including information security tools with tools for coordination, strategic goal-setting, resource allocation and decision-making. The subject of the research is models and methods for comprehensive assessment of information security risks as part of the process of managing information security risks of CII objects based on data mining methods and cognitive modeling technologies. The goal is to increase the reliability and efficiency of technologies and procedures for comprehensive assessment of information security risks of CII objects based on the methodology of cognitive modeling and machine learning methods. To achieve this goal, the following tasks were set and solved: 1. System analysis of the problem of comprehensive risk assessment of information security of CII objects, development of a concept for its solution. 2. Development of problem-oriented models for parameterizing threats and vulnerabilities of CII objects. 3. Development and research of a method and algorithms for qualitative assessment of information security risks of CII objects based on technologies for semantic analysis of text descriptions of threats and vulnerabilities. 4. Development and research of a method and algorithms for quantitative assessment of information security risks of CII objects based on cognitive modeling. 5. Development and research of a method and algorithms for assessing the information security risks of CII objects based on identifying anomalies in their condition using intelligent analysis of time series. 6. Development of the architecture of a research prototype of an intelligent decision support system (IDSS) for assessing the IS risks of CII objects and analysis of the results of using the IDSS in solving a number of applied problems in assessing the level of security of specific industrial facilities and organizations.

Key words: information security; data mining; cognitive modeling; machine learning; anomalies; network attacks; cognitive attacks; semantic analysis.

Язык статьи / Language: русский / Russian.

Об авторе / About the author:

ВУЛЬФИН Алексей Михайлович
ФГБОУ ВО «Уфимский университет науки и технологий», Россия.
Профессор каф. вычислительной техники и защиты информации. Дипл. инженера-программиста (Уфимск. гос. нефтяной техн. ун-т, 2008). Д-р техн. наук по методам и системам защиты информации, инф. безопасности (Уфимск. гос. авиац. техн ун-т, 2022). Иссл. в обл. информ. безопасности, интел. систем, нечеткого и нейросетевого моделирования.
E-mail: vulfin.alexey@gmail.com
ORCID: https://orcid.org/0000-0001-5857-2413
URL: https://www.elibrary.ru/author_profile.asp?id=1051942

VULFIN Aleksey Mikhaylovich
Ufa University of Science and Technologies, Russia.
Professor of the department computer technology and information security. Dipl. software engineer (Ufa State Oil Techn. Uni., 2008). Dr. Tech. Sciences on Methods and Systems of Information Security (Ufa State Aviat. Techn. Uni., 2022). Research in the field of information security, intelligent systems, fuzzy and neural network modeling.
E-mail: vulfin.alexey@gmail.com
ORCID: https://orcid.org/0000-0001-5857-2413
URL: https://www.elibrary.ru/author_profile.asp?id=1051942