ОЦЕНИВАНИЕ И ПРОГНОЗИРОВАНИЕ СОСТОЯНИЯ СЛОЖНЫХ ОБЪЕКТОВ: ПРИМЕНЕНИЕ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Израилов К.Е.[1], Буйневич М.В.[2], Котенко И.В.[3], Десницкий В.А.[4]

Цель исследования: *создание способа оценивания и прогнозирования состояния объектов с нетривиальной внутренней структурой, разнофункциональными элементами и сложными связями между ними. Важной особенностью поставленной цели является независимость ее решения от области функционирования сложных объектов. Ставится задача применения данного подхода в области информационной безопасности.*

Методы исследования: *системный анализ, методы аналитического моделирования, статистические методы и методы машинного обучения, разработка программного кода для реализации алгоритмов оценивания и прогнозирования.*

Полученный результат: *введена онтологическая модель обобщенной предметной области, описывающая основные элементы и их взаимосвязи. Произведен обзор отечественной научной литературы за последние несколько лет и анализ существующих в них решений, а также делается их критериальное сравнение. Разработаны принципы построения инвариантных способов оценивания и прогнозирования. Предлагается схема нового способа оценивания и прогнозирования. Дается описание обобщенных алгоритмов функционирования компонентов оценивания и прогнозирования, а также их применимость для решения задач в области информационной безопасности в интересах противодействия сетевым атакам.*

Научная новизна *заключается в систематизации и достаточно обширном обзоре работ за последние десять лет (в основном за последние пять лет), посвященных оцениванию и прогнозированию объектов, имеющих сложную внутреннюю структуру. Систематизация работ ставит своей целью не только анализ и критериальное сравнение результатов исследований, но и синтез решений, «завязанных» на конкретную область применения. Как следствие, предложен способ оценивания и прогнозирования, который в отличие от аналогичных может работать без учета специфики предметной области, и рассматривается его использование для информационной безопасности.*

Ключевые слова: *информационные технологии, онтологическая модель, критериальное сравнение, принципы построения, гипотетическая схема, обобщенные алгоритмы, сетевая безопасность.*

DOI:10.21681/2311-3456-2022-6-2-21

Введение

Глобальное и повсеместное применение информационных технологий привнесло в современную жизнь множество новых возможностей и инноваций. Большое количество объектов, функционирующих в образовавшейся информационной среде, оказалось связанным по множеству входных и выходных параметров. При этом информационные потоки оказались не только соединяющими отдельные объекты, но и пронизывающими их самих, то есть каждый объект, в свою очередь, стал являться уникальной средой для

1 Израилов Константин Евгеньевич, кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, Санкт-Петербург. ORCHID: https://orcid.org/0000-0002-9412-5693. Scopus Author ID: 56123238800. E-mail: konstantin.izrailov@mail.ru

2 Буйневич Михаил Викторович, доктор технических наук, профессор, профессор кафедры прикладной математики и информационных технологий Санкт-Петербургского университета государственной противопожарной службы МЧС России, Санкт-Петербург. ORCHID: https://orcid.org/0000-0001-8146-0022. Scopus Author ID: 56122749800. E-mail: bmv1958@yandex.ru

3 Котенко Игорь Витальевич, доктор технических наук, профессор, главный научный сотрудник и руководитель лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, Санкт-Петербург. ORCHID: https://orcid.org/0000-0001-6859-7120. Scopus Author ID: 15925268000. E-mail: ivkote@comsec.spb.ru

4 Десницкий Василий Алексеевич, кандидат технических наук, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, Санкт-Петербург. ORCHID: https://orcid.org/0000-0002-3748-5414. Scopus Author ID: 36634098200. E-mail: desnitsky@comsec.spb.ru

внутренней передачи и обработки разнотипных данных. Возникла потребность контроля и оценки объектов не как отдельных узлов, а как представляющих собой сложные объекты (далее – СлО) с внутренней средой и логикой, определяемых в каждый момент времени некоторым состоянием – совокупностью характеризующих его значений. За процедурой же оценивания состояния СлО, логично, следует и процедура прогнозирования его состояний, например, для своевременной замены оборудования на грани неисправности или для превентивного противодействия угрозам.

К настоящему времени наработан значительный научно-методический аппарат с целью обеспечения таких процедур для различных типов и классов СлО с учетом специфики области их применения. Однако, исходя из применимости СлО в огромном количестве областей (транспортных, энергетических, социальных и пр.), возникает настоятельная потребность в едином методологическом аппарате как описания состояний СлО, так и его оценивания и прогнозирования. В противном случае для целого ряда масштабных проектов и технологических платформ (например, компьютерных сетей, Умного города или Интернета вещей, объединяющих и обеспечивающих взаимодействие качественно разных объектов и субъектов [1-4]), поддержанных целым «букетом» специфических моделей, методов и методик, задача оценивания и прогнозирования состояния и «поведения», как результирующей сущности, так и отдельных гетерогенных СлО в ней, становится принципиально не решаемой никаким из известных способов.

С учетом вышеизложенного сформулируем цель настоящего исследования следующим образом:

создание способа оценивания и прогнозирования состояния сложных объектов, инвариантных области их применения.

Здесь и далее под способом в широком смысле слово будем понимать совокупность выбранного метода (базовая модель → собственно метод → схема шагов → методика → алгоритм) решения целевой задачи, средства (используемый математический и программный инструментарий) и формы реализации процесса решения (ручная, автоматическая или совместная):

Способ = Метод + Средство + Форма.

Исходя из методологической сложности цели, первым шагом для ее достижения может быть решение частной задачи в виде аналитического обзора научных публикаций, в которых подобные вопросы уже поднимались (релевантных работ) – именно это и будет сделано в данной статье. В случае, если какие-либо способы будут иметь специализацию в применении, потребуется их обобщение. Как результат, гипотетически уже на этом шаге удастся создать если не сами обобщенные способы оценивания и прогнозирования, то лежащие в их основе принципы. На основании последних можно будет предположить первоначальную схему нового способа, обеспечивающего оценивание и прогнозирование, инвариантного к области применения СлО.

Основным научным вкладом, полученным в результате исследования, является следующее. Во-первых, представлена онтологическая модель текущей предметной области, которая строго вводит основные понятия и их взаимосвязи, на базе чего могут рассматриваться существующие и предлагаются новые способы оценивания и прогнозирования состояния СлО. Во-вторых, сформулированы принципы, которые могут использоваться для построения новых способов, инвариантных к предметной области функционирования СлО. И, в-третьих, предложена схема такого способа, который после разработки и реализации входящих в него алгоритмов может быть непосредственно применен на практике. Также предложено описание четырех основных алгоритмов способа, применимых для области информационной безопасности в части оценивания и прогнозирования состояния сетевых узлов организации под воздействием атак. Доведение алгоритмов до практической реализации позволит создавать механизмы противодействия сетевым атакам качественно нового уровня.

Необходимо отметить, что исследование оценивания и прогнозирования состояния процессов функционирования СлО здесь рассматриваться не будет, так как решения, найденные для СлО, могут быть адаптированы и к ним, поскольку такие процессы можно рассматривать, как временную последовательность состояний СлО.

Статья организована следующим образом. В первом разделе приводится онтологическая модель, вводящая основные понятия предметной области и их взаимосвязь. Во втором и третьем разделах производится обзор научных публикаций российских ученых, релевантных к теме оценивания и прогнозирования состояния СлО. В четвертом разделе делается сравнительный анализ рассмотренных публикаций по нескольким критериям. В результате предлагаются принципы, лежащие в основе единого инвариантного способа оценивания и прогнозирования. В пятом раз-

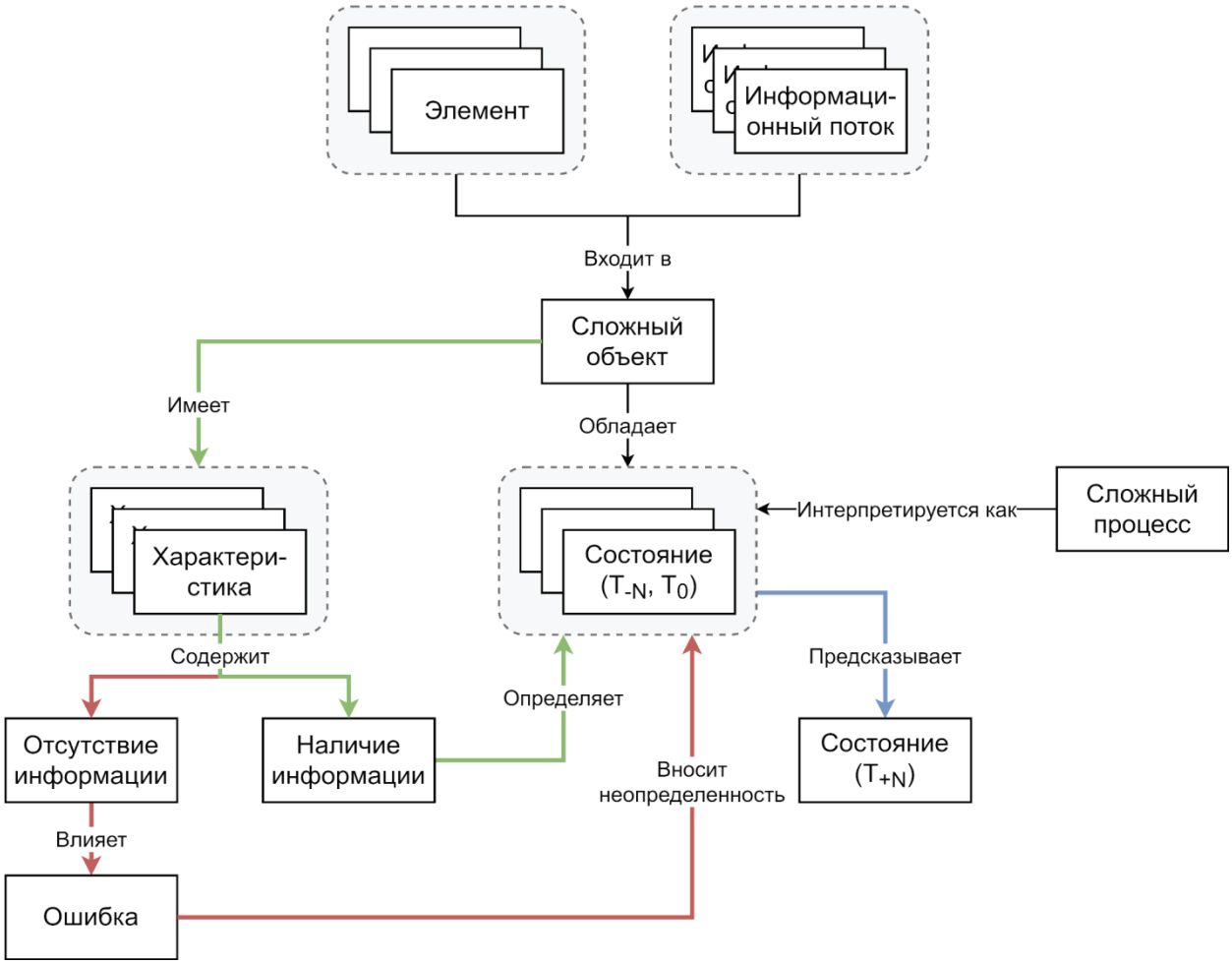

Рис. 1. Онтологическая модель предметной области

деле предлагается гипотетическая схема такого способа. В шестом разделе описываются обобщенные алгоритмы для компонентов оценивания и прогнозирования, указывается их применимость в области информационной безопасности. В последнем разделе подводятся итого проведенного исследования и предлагаются пути его развития.

1. Онтологическая модель

Ввиду того, что цель текущего исследования сама по себе является достаточно сложной для интерпретации (из-за использования не всегда однозначно воспринимаемых терминов, а также неочевидности их взаимосвязей), предложим онтологическую модель предметной области (рис. 1), необходимую для последующего решения задач оценивания и прогнозирования состояния процессов функционирования СлО.

Модель (см. рис. 1) содержит следующие элементы:

1) сложный объект – искусственно созданный объект с нетривиальной внутренней структурой, объединяющей разнофункциональные элементы и информационные потоки между ними;

2) элемент (СлО) – часть структуры СлО, выполняющая заданный функционал;

3) информационный поток – часть структуры СлО, представляющая собой информацию, циркулирующую между элементами СлО;

4) характеристика (СлО) – отличительное свойство, которое *имеет* СлО в заданный момент времени (настоящий или прошедший);

5) наличие информации (о характеристике) – факт достаточности информации, *содержащейся в* характеристике для идентификации состояния СлО;

6) отсутствие информации (о характеристике) – факт недостаточности информации, содержащейся в характеристике СлО (по аналогии с ГОСТ 34100.3-2017 в части «Неопределенность измерений»);

7) ошибка оценивания (состояния СлО) – факт *внесения неопределенности* в состояние СлО, на который *влияет* отсутствие информации о характеристиках

(причины и последствия наличия ошибок отмечены на схеме красным цветом);

8) сложный процесс (СлО) – процесс функционирования СлО, *интерпретируемый как* изменение его состояния с течением времени;

9) состояние (T_{-N}, T_0) – совокупность значений характеристик (т.е. информации), которыми *обладает* СлО в данный и предыдущие моменты времени; в данном случае T_{-N} интерпретируется, как время в N-й момент до текущего момента, а T_0 – текущий момент времени;

10) Состояние (T_{+N}) – совокупность значений характеристик, которыми будет обладать СлО в последующие моменты времени; может быть *предсказано* на основании предыдущих состояний T_{-N} и T_0; в данном случае T_{+N} интерпретируется, как время в N-й момент после текущего момента;

11) состояние сложного процесса – совокупность значений характеристик, *интерпретируемая как* последовательность состояний СлО, расположенная на временной шкале;

12) оценивание состояния (СлО) – процедура определения состояний T_{-N} и T_0 СлО на основании информации о его характеристиках (процесс отмечен на схеме зелеными стрелками);

13) прогнозирование состояния (СлО) – процедура определения состояний T_{+N} СлО на основании предыдущих состояний T_{-N} и T_0 (процесс отмечен на схеме синими стрелками).

Следуя онтологической модели, для оценивания и предсказания состояний требуется сбор и анализ значений (т.е. информации) о характеристиках СлО за предыдущие моменты времени. При этом, пропуски или неточности такой информации будут вести к ошибкам в определении состояний. Состояние же процесса СлО является производной от совокупности состояний СлО.

2. Анализ работ по оцениванию состояния

Произведем анализ работ, в которых излагаются концепции, модели, методы, алгоритмы и иные элементы методологического аппарата, направленные на создание систем оценивания состояния СлО. Для обзора использовалась база Российского индекса научного цитирования[5]. Общее число просмотренных работ составило 300 наименований по запросам, близким к понятию «оценивания состояния сложного объекта». Далее приведен аналитический обзор наиболее «свежих» и релевантных (по мнению авторов настоящего исследования) из них.

Статья [5] посвящена повышению эффективности функционирования сложных информационных объектов, участвующих в работе крупных систем различного назначения. Указывается необходимость оценки как количественных, так и качественных параметров объектов. Состояние сложного объекта в ней оценивается с помощью последовательности следующих шагов:

- сохранение поступивших данных;
- уменьшение размерности данных (например, применением фрактального или корреляционного анализа);
- переход показателей к относительным единицам (например, с применением шкал);
- обобщение показателей по заранее заданным группам с вычислением уровней, характеризующих каждую группу;
- вычисление общего состояния объекта (в статье под этим понимается эффективность функционирования);
- формирование набора решений;
- представление итоговой информации (решений) для лица принимающего решение.

В качестве достоинства авторского решения указана возможность совместной оценки количественных и качественных параметров.

Работа [6] посвящена формированию базы знаний, применимой для оценивания состояния объектов. Основной предпосылкой к исследованию явилось наличие человеческого фактора при осуществлении оценок характеристик. Для повышения ее качества указана необходимость применения систем поддержки принятия решения. В качестве фактора, повышающего точность работы предлагаемых решений приводится адекватность формируемой базы знаний, основой для создания которой явилась нечеткая искусственная нейронная сеть (далее – ИНС).

Суть схемы формирования базы знаний заключается в следующих шагах:

1) выявить особенности характеристик объекта; при этом необходимо учесть разновидность данных, а также возможность их частичного отсутствия (т.е. пропуски и/или неполноту);

2) выбрать вид нечетких правил; в качестве шаблона правил предложена система ограничений на входные переменные (вида «ЕСЛИ Вход_1 = Ограничение_1 ИЛИ … ИЛИ Вход_N = Ограничение_N ТО Выход = Состояние (Вес_Правила)») и ассоциаций с ними выходного значения;

5 http://elibrary.ru

3) создать нечеткую модель ИНС; данный шаг практически совпадает с подобными для классических ИНС и состоит из конструирования топологии, а также инициализации и настройки ее параметров.

Для обучения нечеткой ИНС автором используются генетические алгоритмы. Целью применения последних ставится повышение точности классификации обучающих данных при сохранении точности классификации тестовых данных.

Также в статье описан программный комплекс, реализующий работу с нечеткой ИНС и строящий базу знаний. Тестирование комплекса осуществлялось для выбора нефтяной скважины, исходя из ее параметров, а также информации о нефтяном пласте и параметрах начала отбора (всего 3398 записей по 46 объектам). Результатом работы комплекса явилось получение оценки вероятной эффективности скважины в виде бинарного значения. Перед использованием входных данных применялась их корректировка путем устранения выбросов и аномалий, а затем выявлялись зависимости среди них. Итоговая база знаний состояла из 448-ми нечетких правил и 4-х параметров с 5-ю возможными численными значениями.

Данный подход был применен автором и в задачах из смежных областей – для оценки характеристик водоводов на кустовых насосных станциях [7, 8].

В статье [9] (по аналогии с [6–8]) нечеткая ИНС применяется для оценивания состояния системы электропотребления промышленного объекта. Основной целью такого анализа является предсказание спроса у энергопотребителей в будущем. Данный процесс строится на краткосрочном прогнозировании, что является достаточным для решения данной задачи. Автор показывает, что типичными применяемыми способами решения задач прогнозирования в электроэнергетике являются регрессионные модели, факторный анализ, обобщенное экспоненциальное сглаживание и др. Однако им подчеркнута низкая точность таких решений, для чего как раз и предложено применять нечеткие ИНС. Структура последней состоит из слоя «Вход–Выход», условия «Если» и правила «То»; а каждая такая пара является отдельным нечетким правилом.

В статье [10] решается задача оценивания состояния Интернет-объектов, для чего также предложено применять совокупность нечеткой логики и ИНС. Указано, что данный подход может использоваться для целого ряда классических задач, таких, как идентификация, классификация и кластеризация. Также обоснована применимость подхода и для классификации компьютерных атак. Результаты проведенного эксперимента подтверждают как работоспособность подхода, так и его высокую эффективность.

В статье [11] решается задача выявления дефектов в дорожных покрытиях на основании фото и видео изображений. Обосновано, что ручная работа с параметрами таких СлО будет занимать длительное время. Авторами рассмотрено три решения задачи с использованием сверточных ИНС – Unet, Linknet и PSPNet. В качестве входных данных взят набор Crack500 из открытой базы датасетов Kaggle.

Статья [12] рассматривает СлО, как совокупность однотипных элементов, организующих единую систему взаимодействия. В работе предлагается авторский метод идентификации объектов с применением «горной» кластеризации, состояния которых являются близкими. Это позволяет определять близкие для них отклонения в работе и применять подобные механизмы воздействия. Метод состоит из следующих шагов: формирование списка объектов с отклонениями, выявление кластеров и объектов, близких к центрам кластеров, очистка данных последних, исключение близких объектов, повторение кластеризации и последующих шагов (до момента, когда количество кластеров будет соответствовать количеству объектов), экспертное формирование воздействий. Проведенный численный эксперимент обосновывает работоспособность метода.

В статье [13] ставится методологически важный вопрос касательно возможных подходов к измерению состояния СлО без привязки к какой-либо предметной области. В качестве особенности рассмотрения авторы указывают темпоральность массивов данных (т.е. наличие зависимости от времени), что приводит к траектории их состояний в соответствующем пространстве. Вводится понятие шкалы измерения состояния СлО со множеством переменных, как доли длины вектора, исходящего из точки начала координат и заканчивающегося на опытном объекте. Длина вектора принимается равной расстоянию между двумя опорными состояниями на эталонной прямой в пространстве траекторий. Используемый математический аппарат близок к некоторым подходам из области термодинамики. Он может применяться как основа способа получения признаков для задач, решаемых на базе машинного обучения.

Работы [14, 15] направлены на своевременное выявление различных факторов, негативно влияющих на функционирование сложных автономных технических объектов. Это предлагается достигать повыше-

нием точности оценивания состояния таких объектов в процессе их мониторинга; причем одной из причин снижения точности указывается наличие помех и шумов. Отмечена сложность оценивания СлО, заключающаяся в том, что внешние воздействия могут влиять не только на его параметры, но и на структуру. Также подчеркивается, что процесс контроля может вести к снижению качества измерения параметров, что увеличивает неточность в оценке объекта. Для решения озвученных задач предлагается применять метод вейвлет-преобразований, качественно отличный от других методов (выявление аномалий и локальных особенностей, фильтрация и пр.). Эти преобразования могут формировать признаковое пространство сложного объекта, за которым логично последует использование методов классификации. Авторы делают краткий обзор последних, выделяя для них следующую методологическую, признаковую и инструментально-математическую базу: оценивание состояния не на интервале, а на области неопределенности выходных параметров; применение нечеткой логики и анализа иерархий, сравнение измеренных параметров с предопределенными, статистическая классификация, ИНС, интеллектуальные агенты, вейвлет-преобразования. Среди сделанных обзоров работ отдельно выделяется именно применение вейвлет-преобразований, имеющих целый ряд преимуществ.

Состояние сложного объекта предлагается определять, как набор его параметров в некоторых заданных границах. Само распознавание классов состояния сложного объекта состоит из следующих шагов: создание базы данных о нормальных и аномальных состояниях, определение уравнений классификатора, разложение информации на вейвлет-коэффициенты, поиск информативных признаков, определение области работоспособности и самого состояния объекта, корректировка состояния с учетом ошибок, получение класса состояния, расчет метрик определения состояния, вычисление эффективности управления состоянием технического объекта. Интеллектуализация обеспечивается применением в архитектуре системы оценивания модулей базы знаний с правилами принятия решений, самого решателя задачи на основании правил, человеко-ориентированной аргументации действий и общей базы данных.

3. Анализ работ по прогнозированию состояния

Аналогично оцениванию состояния СлО и используя аналогичные условия отбора, произведем обзор работ, посвященных прогнозированию состояния СлО.

В статьях [16, 17] поднимается и решается задача моделирования сложных технологических объектов, для чего предлагается применять методы машинного обучения. При этом оценивание состояния и прогнозирование (аналогично работе [9]) рассматриваются в едином аспекте. Так, общая схема обработки информации представляет собой два слоя: первый состоит из ансамбля сверточных ИНС и производит оценивание состояния объекта, а второй – из одной ИНС такого же типа, получает на вход результаты работы первого слоя и осуществляет прогнозирование состояния объекта. Для проверки работоспособности подхода в части оценивания состояния использовалось распознавание изображений алюминиевых сплавов для определения их агрегатного состояния. Проверка подхода в части прогнозирования состояния не проводилась, однако авторы обосновывают работоспособность подхода и в этом случае.

Статья [18] имеет цель, заключающуюся в прогнозировании технического состояния локомотивного оборудования с применением ИНС. Это позволит заранее планировать ремонтные и иные обслуживающие работы. В качестве типов сетей выбраны качественно разные – прямого распространения и рекуррентная. Архитектура первой сети являлась однослойной с 300 нейронами и глубиной погружения 12 в хронологию данных; цикл обучения составил 600 эпох. Архитектура второй сети представляла собой один LTSM-слой из 512 нейронов и глубиной погружения 14; цикл обучения составил 150 эпох.

Результаты эксперимента на данных от системы смазки дизеля тепловоза показали, что ИНС прямого распространения позволяет предсказывать состояние не более чем на 3 суток, что является недостаточным – минимально необходимым сроком считается 25 суток; при этом увеличение срока предсказания ведет к существенному нарастанию ошибок. Как альтернатива, рекуррентная ИНС на отметке в 30 суток с момента последних измерений имеет ошибку в диапазоне 3–5%, что считается хорошим результатом для подобного рода задач.

Статья [19] посвящена реализации системы IDAS (сокр от *аббр. от англ.* Intelligent Driver Assistance System – Интеллектуальная Система Помощи Водителю). В качестве решения предлагается совместить два подтипа рекурентных ИНС – с длинной и кратковременной памятью, которые объединяются с нечеткой ИНС (используемой, если текущая ситуация не похожа ни на одну нештатную). Входными данными является информация от видеорегистраторов; скорость же реа-

гирования системы составляет менее 1 секунды.

Шаги работы в упрощенном виде являются следующими (с указанием примера применяемых алгоритмов): выделение подвижных объектов в области видимости (алгоритмы обработки изображений SURF и кластеризации особых точек DBSCAN); определение типа объекта (рекуррентная ИНС); определение типа нештатной ситуации (нечеткая ИНС); формирование решения для выхода из ситуации (заданные правила).

Рекурсивная ИНС состояла из 512 LTSM-ячеек. Эксперименты с прототипом, реализующим предложенный подход, показали его общую работоспособность и приемлемую эффективность. Однако авторы отмечают, что модели требуют улучшения и большего количества данных для обучения.

Статья [20] направлена на исследование возможностей применения методов машинного обучения для прогнозирования состояния объектов, описываемых произвольным числом параметров. В работе рассматривается классическая задача предсказания будущего класса состояния объекта, имеющего два значения (интерпретируемого, например, для технических устройств, как исправен или сломан). Текущее и предыдущие состояние объекта описываются в виде временного ряда из значений одинакового набора параметров. Таким образом, весь набор данных представляет собой таблицу, где столбцами, кроме последнего, являются состояния объекта с временными метками, строками – значения параметров для каждого состояния, а последним столбцом – класс состояния. На основании этого, авторами разработан и протестирован программный прототип, реализующий традиционные методы машинного обучения и производящий оценку полученной модели. В качестве классификаторов реализованы такие алгоритмы, как логистическая регрессия, дискриминантный анализ, классификатор Байеса, ИНС, SVM, бэггинг деревьев решения, а также их агрегация. Для оценки качества модели машинного обучения вычисляются F-мера и площадь под графиком ROC-кривой. Эксперименты с прототипом показали, что для разных задач наилучшими могут оказываться различные классификаторы и их комбинации.

Работа [21] направлена на оценивание технического состояния СлО – авиационного двигателя – как в текущем состоянии, так и в некоторый будущий момент времени; в качестве предсказания берется промежуток до следующей проверки устройства. Для решения этой задачи предлагается применять цепи Маркова первого порядка. Так, вычисляется вероятность того, что некоторый оцениваемый параметр по истечению времени выйдет за допустимые границы, что будет означать его прогнозирование. Данную оценку можно расширить и на весь вектор параметров, говоря, таким образом, о прогнозировании состояния всего СлО. Также необходимо учесть случайный характер изменения параметра при переходе из текущего состояния в следующее. Предложенный подход позволяет оценить вероятность и оптимальное время выхода наблюдаемого объекта за допустимые границы, что имеет особую актуальность при обслуживании воздушных судов. Подобные идеи развиваются другими авторами: в работе [22] – для прогнозирования состояния парка автомобилей и в [23] – для прогнозирования развития пожара.

4. Анализ представленных работ

Систематизируем результаты, полученные из проведенного обзора, в виде табл. 1, содержащей, помимо информации о самих статьях, их соответствие следующим критериям, релевантным текущей задаче исследования (с указанием возможных значений):

1) K_1 – решается ли задача оценивания состояния СлО: «+» – да, «–» – нет, «0» – частично;

2) K_2 – решается ли задача прогнозирования состояния СлО: «+» – да, «–» – нет, «0» – частично;

3) K_3 – применяется ли машинное обучение: «+» – да, «–» нет;

4) K_4 – стадия решения задачи: «Т» (*аббр*. от Теория) – решение рассмотрено только теоретически, «Э» (*аббр*. от Эксперимент) – создан прототип и проведены эксперименты, «П» (*аббр*. от Практика) – решение имеет готовый вид, применимый практически;

5) K_5 – абстрактность данных по отношению к предметной области, в которым применяется решение: «+» – не зависят, «–» – учитывают специфику;

6) K_6 – применяемые математический аппарат и приемы: 1 – уменьшение размерности (фрактальный или корреляционный анализ); 2 – обобщение; 3 – переход к относительным единицам; 4 – нечеткая ИНС; 5 – генетический алгоритм; 6 – сверточная ИНС; 7 – кластеризация; 8 – пространство состояний; 9 – вейвлет-преобразование; 10 – классическая ИНС прямого распространения; 11 – рекуррентная ИНС; 12 – классификаторы и алгоритмы регрессии, кроме ИНС; 13 – цепи Маркова 1-го порядка.

Значение K_1 равное 0 (т.е. «частично») означает, что хотя статья и посвящена прогнозированию состояния СлО, однако в ней неявно осуществляется и его оценивание. Аналогично, значение 0 для K_2 означает,

Таблица 1

Критериальное сравнение результатов обзора научных статей

№ Гр.	№ Ст.	Ссылка	Название	Год	К_1	К_2	К_3	К_4	К_5	К_6
1	1	[5]	Информационная система оценки состояния сложного объекта	2016	+	–	–	Т	+	1, 2, 3
2	2	[6]	Нейронечеткая модель и программный комплекс формирования баз знаний для оценки состояния объектов	2022	+	0	+	П	+	4, 5
	3	[7]	Нейронечеткая модель и программный комплекс автоматизации формирования нечетких правил для оценки состояния объектов	2019				П		
	4	[8]	Нейронечеткая модель формирования нечетких правил для оценки состояния объектов в условиях неопределенности	2019				П		
3	5	[9]	Оценка и прогнозирование состояния систем электропотребления промышленных объектов	2013	+	0	+	Э	–	4
4	6	[10]	Автоматизация процедур мониторинга в Web-пространстве на основе нейро-нечёткого формализма	2015	+	0	+	Э	–	4
5	7	[11]	Применение семантических сверточных нейронный сетей для детекции трещин дорожного покрытия	2021	+	0	+	Э	–	6
6	8	[12]	Идентификация состояния сложного объекта на основе анализа сигнатуры его состояния	2020	+	–	+	Э	+	7
7	9	[13]	Построение шкал для измерения состояний сложных объектов в многомерных пространствах	2018	+	0	–	Т	+	8

DOI:10.21681/2311-3456-2022-6-2-21

№ Гр.	№ Ст.	Ссылка	Название	Год	К_1	К_2	К_3	К_4	К_5	К_6
8	10	[14, 15]	Интеллектуальное оценивание технического состояния сложных технических объектов	2021	+	0	–	Э	+	9
9	11 12	[16] [17]	Применение глубоких нейронных сетей в моделях сложных технологических объектов Модели сложных технологических объектов на основе сетей глубокого обучения	2020 2019	+	+	+	Э Т	–	6
10	13	[18]	Предиктивная аналитика технического состояния систем тепловозов с использованием нейросетевых прогнозных моделей	2021	–	+	+	П	–	10, 11
11	14	[19]	Система ситуационного управления и контроля плохо формализуемых сценариев динамических сцен	2018	0	+	+	Э	–	4, 7, 11
12	15	[20]	Прогнозирование состояния технического объекта с применением методов машинного обучения	2019	0	+	+	Э	+	10, 12
13	16 17 18	[21] [22] [23]	Прогнозирование технического состояния авиационных двигателей при их эксплуатации по состоянию Применение марковских цепей для прогнозирования состояния парка автомобилей в моделях с дискретным состоянием и непрерывным временем Применение марковских цепей для моделирования и прогнозирования развития пожара	2011 2022 2021	+	+	–	Т Э Т	–	13

Примечание. В таблице используются следующие обозначения: «№ Гр.» – номер группы публикаций с близкими тематиками, «№ Ст.» – номер статьи, «Ссылка» – библиографическая ссылка на статью, «Год» – год публикации статьи. В случае группировки нескольких статей, ссылка название и год, а также К_4 и К_6 указываются для каждой, а остальные критерии – для всей группы.

что оценивание состояния делается как часть или в интересах прогнозирования. Также, из всех публикаций, близкие по смыслу работы объединены в 13 групп.

Исходя из проведенной систематизации (см. табл. 1) можно сделать следующие выводы (согласно датам публикаций и выбранным критериям).

Во-первых, хотя задача оценивания и прогнозирования состояния СлО решается уже достаточно давно (первая рассмотренная публикация датирована 2011 годом), однако ее актуальность существенно увеличилась именно в последние 5 лет (с 2018 по 2022 год присутствуют 14 публикаций, включая близкие).

Во-вторых, из всех 13 групп публикаций только одна формально не относится к оцениванию состояния СлО, две относятся частично, а десять – полностью. Из всех групп публикаций только в двух не предполагается явно использовать оценивание состояния СлО для его последующего прогнозирования, в шести используются частично, а пять работ напрямую посвящены задаче прогнозирования. Таким образом, оценивание состояния СлО зачастую осуществляется для прогнозирования. Следовательно, эти задачи являются смежными, поэтому могут строиться на единой основе.

В-третьих, примерно в 30-ти % групп (точнее, в 4-х из 13-ти) машинное обучение не применяется для оценивания и прогнозирования. Так, в 3-х исследованиях из 4-х предлагается оценивать состояние СлО следующим образом: переходом к относительным единицам с обобщением и ранжированием состояний; использованием пространства состояний, «взятого» из термодинамики; применением вейвлет-преобразований. Для прогнозирования же состояний указывается возможность использования цепей Маркова первого порядка.

В-четвертых, из всех работ (т.е. из 18-ти) ровно половина доведена до эксперимента, а другие или рассматривают только теоретические аспекты – четыре работы, или уже имеют практическую реализацию – пять работ. Такая закономерность может быть объяснена тем, что любая теоретическая база оценивания и прогнозирования СлО достаточно часто может быть доведена до реального работающего прототипа, однако доведение его до готового продукта (включающего, видимо, этапы полномасштабного тестирования, оптимизации и повышения юзабилити) имеет ряд существенных сложностей.

В-пятых, чуть меньше половины групп работ (6 из 13-ти) оперирует данными достаточной степени абстрактности, позволяя применять решения практически для любой предметной области. Таким образом, далеко не во всех случаях требуется специализация моделей и методов (например, ИНС) для конкретной задачи.

И, в-шестых, набор применяемых математических подходов и приемов крайне многообразен: из 13-ти групп статей лишь малая часть имеет пересечения: в четырех работах применяется нечеткая ИНС, также в четырех работах – сверточная ИНС, кластеризация, классическая ИНС прямого распространения и рекуррентная ИНС, в остальных же работах используются частные подходы, например, цепи Маркова в [21, 22]. Следует отметить подходы, основанные именно на ИНС, которые, видимо помимо общей популярности, обеспечивают достаточно высокую результативность оценивания и прогнозирования. Таким образом, при незначительном многообразии применяемых подходов все же прослеживается доминанта – ИНС.

Исходя из проведенного анализа, а также применяя имеющийся у авторов опыт создания различного рода концепций, моделей и парадигм, можно сформулировать нижеследующие принципы, лежащие в основе инвариантного способа оценивания и прогнозирования состояния СлО (с указанием критериальных и иных предпосылок к каждому из принципов) [1, 2, 24, 25, 27-29]:

1) П_1, принцип ***единства*** (моделирования состояния и (или) оценки ситуационной осведомленности) – «Процессы оценивания и прогнозирования должны представлять части единого процесса, который может быть обобщенно назван *моделированием состояния СлО* и (или) оценки ситуационной осведомленности о СлО. В основе же процессов должна лежать общая модель» (из К_1 и К_2);

2) П_2, принцип ***междисциплинарности*** (подходов) – «Математический инструментарий процессов оценивания и прогнозирования не обязан строиться исключительно на машинном обучении или другом частном подходе, а должен применять несколько методов и междисциплинарный подход» [26] (из К_3 и К_6, а также на основании [27, 28]);

3) П_3, принцип (повышения) ***эффективности*** (процедур) — «При создании моделей и методов оценивания и прогнозирования состояния СлО должны быть учтены возможности по повышению эффективности процедур — улучшение результативности, снижение времени работы, экономия ресурсов» (из К_4 и авторского опыта [29]);

4) П_4, принцип ***абстрактности*** (данных) – «Модели и методы оценивания и прогнозирования состояния СлО должны строиться на абстрактных данных, но с возможностью формирования решений, учиты-

вающих специфику любой требуемой предметной области» (из К_5);

5) П_5, принцип ***тождественности*** (методов) – «Сложный процесс можно рассматривать, как последовательность состояний СлО, и применять к нему тождественные методы оценивания и прогнозирования» [30];

6) П_6, принцип ***адаптации*** (состояний) – «В условиях недостаточности и неопределенности данных должна происходить адаптация состояний в процессе анализа новых значений характеристик СлО» (из специфики задачи [31], общего анализа и опыта авторов);

7) П_7, принцип ***обусловленности*** (форм характеристик) – «Выбор формы характеристик СлО, а также их содержимого и допустимых границ, должен основываться на закономерностях среды (как правило, всего физического мира), в котором данный СлО функционирует» (из общеизвестной практики [32] и опыта авторов [2, 33]).

Дадим небольшое уточнение касательно принципа 7, поскольку он на первый взгляд противоречит принципу 4. Имеется в виду, что без учета привязки к предметной области, любой объект подчиняется законом мира, в котором он существует. Следовательно, свойства и поведение объектов в реальном мире описываются его физическими законами [34], что может быть использовано для интерпретации характеристик СлО, оценивания его состояния и прогнозирования поведения [35]. Так, например, у любого реально существующего объекта есть понятия размера, местоположения и температуры, измеряемые значения которых не могут быть произвольными [36] – размер всегда больше 0, местоположение больше или равно 0, но менее размеров окружающей местности (в пределе – окружность Земли или ее диаметр); температура больше (а теоретически и равна 0) градусов Кельвина, но не более предельной на Земле (около миллиона Кельвинов) [37, 38] и т.д. Таким образом, проанализировав возможные значения некоторой характеристики и логику ее изменения, можно предположить ее контекстный (как правило, физический) смысл, определить возможную динамику изменения, допустимые границы и, как следствие, аномальные состояния СлО.

5. Схема инвариантного способа оценивания и прогнозирования

Используя сформулированные выше принципы, предположим следующий способ оценивания и прогнозирования состояния СлО, обладающий инвариантностью к области применения.

Идея способа заключается в построении модели переходов между состояниями СлО с ее итеративным уточнением по мере получения новых значений характеристик – таким образом будет обеспечиваться не только параметрический, но и структурный синтез системы состояний СлО. Используя данную модель, для которой классически применяется граф переходов, очевидно, возможно и вероятностное прогнозирование последующих состояний. При этом, состояние строится на основании отнормированных характеристик СлО (соответствующих его модели в текущей момент времени T_0); при определении состояния используются независимые от предметной области правила, а в случае отсутствия близкого по параметрам состояния СлО создается новое. Также применяется ряд динамических корректировок (т.е. действующих по мере получения новой информации о динамике функционирования СлО), таких, как уточнение модели СлО, правил идентификации состояний, оптимизация модели состояний; при ошибочном прогнозировании модель также корректируется соответствующим образом. Первоначальная схема такого способа представлена на рис. 2.

На схеме (см. рис. 2) для части элементов указано их соответствие предложенным принципам (в полукругах с красным фоном); соответствие П_2 определяется тем, что как для оценивания, так и для прогнозирования не указаны конкретные применяемые подходы (например, в первом случае может использоваться машинное обучение в части классификации, а во втором – марковские сети или же наоборот). Элементы с зеленым фоном относятся к процессу оценивания, а с синим фоном – к процессу прогнозирования. Пунктирной красной линией обозначен начальный элемент схемы, а сплошной красной линией – основная ветка работы схемы (от источника данных, до оценивания текущего состояния и прогнозирования последующего). Интерпретация элементов схемы следующая (сначала основная ветка, затем все дополнительные):

1) окружающий мир – мир, в котором функционируют множество СлО;

2) поток измерений – множество измерений над СлО в последовательные моменты времени;

3) набор характеристик – совокупность характеристик СлО, отражающих его свойства в некоторый момент времени;

4) нормировка характеристик – перевод значений характеристик в инвариантные величины, независящие от единиц, диапазонов измерений и т.п.; может

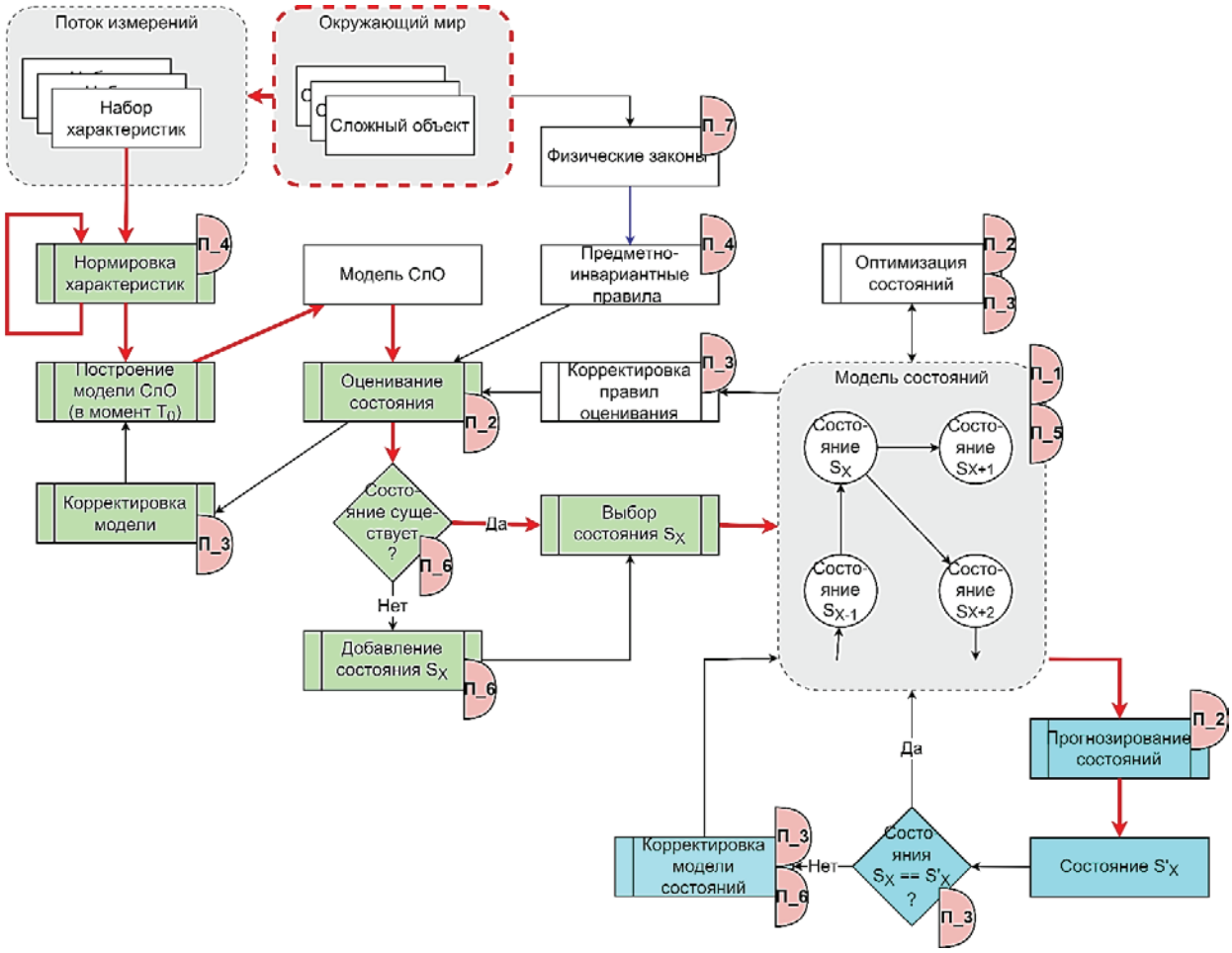

Рис. 2. Схема способа оценивания и прогнозирования состояния сложного объекта

корректироваться по мере сбора статистической информации о характеристиках;

5) построение модели СлО (в момент T_0) – построение статического представления СлО в текущей момент времени;

6) модель СлО – некоторое статическое представления СлО на базе его характеристик (например, в виде списка значений отнормированных характеристик);

7) оценивание состояния – термин описывался выше (см. рис. 1, элемент 12 онтологической модели);

8) «Состояние существует?» – проверка того, что идентифицированное состояние СлО уже присутствует в модели состояний;

9) выбор состояния S_X – выбор текущего состояния СлО из присутствующих в модели состояний;

10) модель состояний – представление состояний СлО (в виде графа), отражающее как все такие состояния, так и возможные переходы между ними;

11) состояние S_{X-1}, S_X, S_{X+1}, S_{X+2}, … – все возможные состояния СлО, построенные в процессе получения информации о СлО за предыдущие моменты времени;

12) прогнозирование состояния – термин описывался выше (см. рис. 1, элемент 13 онтологической модели);

13) состояние S'_X – состояние, предсказанное как следующее за S_X;

14) физические законы – законы функционирования окружающего мира, в котором существуют СлО;

15) предметно-инвариантные правила – правила, следующие из физических законов мира, которые не зависят от предметной области СлО;

16) корректировка модели – уточнение модели СлО согласно состояниям, получаемым на основании оценивания;

17) корректировка правил оценивания – уточнение правил, по которым происходит оценивание состояния СлО согласно изменениям в модели состояний;

18) добавление состояния S_X – создание нового состояния СлО и внесение его в модель состояний;

19) оптимизация состояний – оптимизация графа модели состояний, например, объединение близких состояний или удаление лишних (аномальных);

20) «Состояния S_x == S'_x?» – проверка, насколько успешной оказалось прогнозирование состояния СлО по имеющейся модели состояний;

21) корректировка модели состояний – уточнение модели состояний для улучшения ее прогностических возможностей (например, формирование новых переходов между состояниями).

Для объяснения принципа работы схемы способа приведем следующий мысленный эксперимент. Предположим, что СлО является резервуаром для кипячения воды, в котором установлено два датчика – температуры жидкости и включения нагревательного элемента. Весь процесс функционирования резервуара заключается в ручном (т.е. непериодическом) включении нагревательного элемента, автоматическом ожидании достижения температуры 100 градусов и выключении элемента. Естественно, что данный пример является упрощённым, поскольку в реальном СлО будет существенно большее количество датчиков и в разы более сложные взаимосвязи между их показателями. Также опустим тот момент, что данная задача могла бы быть решена (т.е. произведено оценивание и прогнозирование состояний) с помощью машинного обучения в части классификации и регрессии – пример приведен исключительно для применения на нем схемы способа.

В качестве потока измерений будут наборы значений двух характеристик – температуры $Temp$ (значения, для простоты, целые, от абсолютного нуля в –273 градусов до температуры кипения в 100 градусов) и включения $Power$ (булевское значение в виде «1» или «0»). Модель такого СлО может представлять собой пару значений – $<Temp, Power>$. Для лучшей понятности опустим нормировки характеристик, хотя это действие и можно было бы применить для $Temp$ путем постепенного перевода значений в диапазон от 0 до 1. Исходя из изменений этих значений и применяя предметно-инвариантные правила физического мира, как раз и можно предположить, что первый параметр относится к температуре и не превышает 100 градусов, а второй – булевская величина. В первые моменты измерений будет создано некоторое количество состояний, определяемых парой $<Temp, Power>$, значения первого элемента которой быстро бы росли до 100 при значении второго, равного 1 (нагревание воды), и медленно уменьшались при значении второго, равного 0 (остывание воды). Тогда, модель состояний представляла бы собой цикл из множества состояний – сначала соответствующих нагреву, а затем остыванию с переходом снова на нагрев. Однако, по мере повторения процессов нагревания и охлаждения, а также применения оптимизационных методов над моделью, все состояния будут сведены к нескольким, которые могут интерпретироваться как следующие 6 (с указанием значений $Temp, Power$ для состояния):

1) «остывшая жидкость» $\langle 0, 0 \rangle$;
2) «включение нагрева» $\langle 0, 1 \rangle$;
3) «нагрев» $\langle > 0$ и $< 100, 0 \rangle$;
4) «достижение кипения» $\langle 100, 1 \rangle$;
5) «отключение нагрева» $\langle 100, 0 \rangle$;
6) «остывание» $\langle > 0$ и $< 100, 0 \rangle$.

Сам же граф в модели состояний будет следующим циклом: «1) → 2) → 3) → 4) → 5) → 6) → 1)».

Так, например, многократно повторяющаяся закономерность перехода из состояния $\langle 1,1 \rangle$ (нагрев воды с температурой 1 градус) в состояния $\langle 2,1 \rangle$ (нагрев воды с температурой 2 градуса) может быть заменена на единое состояние $\langle 1$ или $2,1 \rangle$ (нагрев воды с температурой от 1 до 2 градусов).

Используя конечную форму модели СлО, будет производиться отнесение СлО к одному из шести данных состояний (естественно, без смысловой интерпретации процесса, поскольку способ не учитывает предметно-ориентированную специфику). Прогнозировать же состояния СлО можно по графу модели состояний (в том числе, применяя вероятностные оценки).

Интересно также сразу отметить возможность выявления аномального поведения информационного состояния СлО, которое в реальном мире может привести к существенным физических последствиям. Так, если после состояния 4) последует снова состояние 4) и при этом многократно, то «наложение» данного феномена на физическую сущность СлО будет означать, что после закипания воды продолжается ее нагрев, потенциально ведущий к ее выкипанию и/или выходу из строя нагревательного элемента с возможным последующим возгоранием. Данная ситуация будет описываться частью графа модели состояний «... → 3) → 4) → 4) ...» и может считаться аномальной по отношению к изначальному графу, построенному на длительном промежутке измерений.

6. Разработка обобщенных алгоритмов оценивания и прогнозирования для информационной безопасности

В качестве первого этапа для обоснования работоспособности инвариантного способа оценивания

и прогнозирования был разработан набор обобщенных алгоритмов, лежащих в основе его схемы. В качестве области применения получаемых решений (с учетом «принципа абстрактности») была взята сетевая безопасность. В этом случае под СлО понимается сетевая инфраструктура организации, под решаемыми на базе способа задачами – обеспечение информационной безопасности организации путем защиты ее сети, под состоянием СлО – значение показателей ее сетевого обмена (как прямых, так и производных), и под оцениванием и прогнозированием состояния СлО – определение показателей сетевого обмена в инфраструктуре организации в текущий и последующие моменты времени. Классическим же подходом по обеспечению сетевой безопасности, в основе которого должен лежать и предлагаемый инвариантный способ, является поэтапное построение модели атак (как правило, графовой) с определением по ней текущего состояния сетевой инфраструктуры и «предсказанием» развития атак, за которым должны следовать превентивные меры противодействия.

Выделено четыре класса основных алгоритмов, реализующих оценивание и прогнозирование состояния СлО:

- предварительной обработки сырых и нечетких данных;
- извлечения знаний из собираемых наборов данных;
- оценивания текущего состояния сложных объектов и процессов;
- прогнозирования состояний сложных объектов и процессов.

Рассмотрим описание этих алгоритмов с указанием реализуемых ими элементов схемы (см. рис. 2), а также их применимость для области информационной безопасности.

Алгоритм предварительной обработки сырых и нечетких данных предназначен для работы с подаваемыми на вход наборами данных и включает в себя коррекцию их типов, а также устранение неполноты и мультиколлинеарности данных о сложных объектах или процессах. При этом подаваемые на вход данные должны представляться в табличном виде, а пользователь может как управлять процессом работы алгоритма (задавать пороговые значения, критерии и т.п.), так и взаимодействовать с алгоритмом по принципу черного ящика. Элементами схемы, для которых предназначен алгоритм, являются «Нормировка характеристик», «Построение модели СлО (в момент T_0)», «Модель СлО» и «Корректировка модели». Данный алгоритм основывается на таких математических соотношениях как проверка пороговых значений, семантический анализ, кластеризация, усреднение, корреляция и дисперсионный анализ. Коррекция типов данных происходит на основе статистических критериев, связанных с количеством уникальных значений признака, обнаружением последовательностей значений признака, анализом текстовых названий признаков, а также анализом дробных значений для представления некорректных из них в качестве целочисленных.

На первом этапе обеспечения сетевой безопасности должен выполняться сбор информации о сетевом трафике (включающем в том числе и вредоносную активность) и представление ее в едином виде, готовом для последующей обработки. При этом, часть данных может отсутствовать, часть – иметь незначимые, в контексте решаемой задачи, отклонения, а часть было бы более результативно представлять в виде производных показателей (т.е. полученных аналитически из основных). В этом случае применение данного алгоритма позволит повысить полноту обрабатываемой сетевой информации, усреднить некоторые показатели, создать дополнительные метрики. Например, если часть сетевых пакетов будет потеряна или сессии не будут корректно завершены, то алгоритм сможет восполнить недостающий сетевой трафик и добавить отсутствующие детали сессии. При получении большого числа мало отличающихся показателей, таких, как скорость передачи данных в локальной сети, они смогут быть заменены одним значением. Также, появится возможность оперировать производными показателями сетевого трафика, например такими, как диапазоны открытых сетевых портов, количество соединений с одним узлом, наличие запросов на открытие сессии, количество потерянных пакетов. Все это позволит получать всестороннюю информацию о поведении участников сетевого обмена, и, как результат, детектировать атаки еще на первых шагах.

Алгоритм извлечения знаний из собираемых наборов данных предназначен для извлечения фрагментов знаний, имеющихся в данных о СлО, в виде ассоциативных правил (вида «ЕСЛИ <посылка>, ТО <следствие>»), содержащих в правой части (следствии) метку класса. В случае, если обрабатывается непрерывная измерительная информация, то в левой части (посылке) используются коэффициенты дискретного вейвлет-преобразования, производимого с использованием ортогональных базисных вейвлет-функций. Элементами схемы, для которых предназначен этот алгоритм, являются «Оценивание состояния»,

«Состояние существует?», «Добавление состояния S_X» и «Модель состояний».

На втором этапе обеспечения сетевой безопасности определяется возможное поведение участников сетевого обмена, как легальных, так и нарушителей; для этого, как правило, строится соответствующая графовая модель. Применение данного алгоритма на большом наборе входных данных о сетевом трафике как раз и позволит построить такую модель, поскольку она будет являться результатом извлечения знаний о нормальных и атакующих воздействиях. Так, если алгоритм определит, что после некоторой нормальной комбинации показателей (или даже их последовательности) сетевой активности следует ситуация, которая считается целью сетевой атаки, то в модели будет отражен данный переход между двумя состояниями, второе из которых будет иметь соответствующую отметку (назовем ее – «под атакой»). В качестве примера можно привести сценарий злоумышленника, который производит постепенный «взлом» сетевых узлов с целью повышения на них привилегий и распространения своих действий далее. Первоначальной целью такой атаки может быть заражение узлов для проведения распределенной DoS-атаки. Данный сценарий после применения алгоритма будет иметь представление последовательности состояний «под атакой», частично связанных переходами с нормальными состояниями. Таким образом, в модели состояний отразится логика поведения всех сетевых участников, извлеченная из сетевого трафика.

Алгоритм оценивания текущего состояния сложных объектов и процессов предназначен для автономного оценивания текущего состояния СлО, включающего наличие или отсутствие в текущий момент определенного вида функциональных неисправностей, дефектов и атакующих воздействий, свойственных целевой системе. Алгоритм строится на основе глубокой ИНС прямого распространения сигнала, обучение которой производится на объединенном наборе данных, полученном из открытых источников и включающем данные о функционировании нескольких видов систем СлО. Элементы схемы, для которых предназначен этот алгоритм, включают элементы для предыдущего, поскольку алгоритмы в рамках предложенной схемы способа (см. рис. 2) должны работать параллельно. Так, первоначальное представление модели состояний строится путем извлечения новых знаний из данных, а последующие – путем сравнения состояний с присутствующими в модели и, при необходимости, расширения последней. Также, для алгоритма предназначены два дополнительных элемента схемы – «Выбор состояния S_X», «Оптимизация состояний», поскольку помимо обновления модели состояний происходит выбор того, который соответствует текущему набору входных данных.

Третий этап обеспечения сетевой безопасности, в отличие от первых двух подготовительных, относится к разряду основных. В процессе его выполнения определяется текущее состояние сетевой инфраструктуры организации, которое, как правило, показывает ее нормальность или подверженность атакам. Данный алгоритм как раз и предназначен для определения такого состояния, а применение ИНС позволит автоматизировать этот процесс, снизив влияние человеческого фактора (в случае привлечения экспертов по сетевой безопасности). Так, например, если в модели отражены все возможные комбинации показателей сетевого трафика, то результатом будет определение того, не происходит ли целенаправленная распределенная DoS-атака с применением различных техник: множественного открытия сетевых соединений, отправки большого количества эхо-запросов, исчерпании доступных портов узла и т.п. При этом признаки каждой из этих техник будут отражаться в модели в виде соответствующего состояния.

Алгоритм прогнозирования состояний сложных объектов и процессов предназначен для автономного прогнозирования состояний сложных объектов и процессов, включающего наличие или отсутствие в некоторый момент времени в будущем определенного вида функциональных неисправностей, дефектов и влияния как непреднамеренных воздействий, так и преднамеренных (атакующих) воздействий, свойственных целевой системе. Элементами схемы, для которых предназначен алгоритм, являются «Прогнозирование состояния», «Состояние S'X», «Состояния SX == S'X?» и «Корректировка модели состояний». Данный алгоритм строится на основе рекуррентной глубокой ИНС, обучение которой производится на семействе наборов данных, полученных из открытых источников и включающих данные о функционировании нескольких видов индустриальных систем. Наличие большого числа гиперпараметров и настраиваемых весов, свойственных для глубоких ИНС, позволяет с достаточно высоким качеством выявлять закономерности между признаками прогнозируемого состояния системы и ожидаемой меткой его класса.

Четвертый этап обеспечения сетевой безопасности, носящий прогностический характер, предназначен для определения будущих состояний по после-

довательности предыдущих, т.е. уже свершившихся. Данный алгоритм предназначен для решения задачи этапа, в том числе и путем применения рекуррентной ИНС. Так, если модель с помощью последовательности состояний будет отражать стадии некоторого сетевого процесса, то находясь в начальных стадиях (что определяется с помощью предыдущего алгоритма), можно спрогнозировать переход сетевой инфраструктуры и в последующие, имеющие отметку «под атакой». Например, если рассматриваемым процессом является распределенная DoS-атака, проводимая путем последовательного «взлома» и заражения сетевых узлов с последующей массовой рассылкой сетевых пакетов, то принять превентивные меры возможно будет уже при первых атаках на узлы сети.

Заключение

В работе представлен подход к решению задачи мониторинга состояния СлО без привязки к конкретной предметной области. Для этого, из-за отсутствия каких-либо универсальных и окончательно сформированных решений, был выполнен анализ публикаций, посвященных вопросам оценивания и прогнозирования состояния СлО. Результаты анализа систематизированы в табличном виде по ряду критериев. Выводы, сделанные в результате таблично-критериального анализа, позволили выделить и сформулировать основные принципы, по которым возможно построение моделей и методов оценивания и прогнозирования состояния СлО, инвариантных области их применения. Исходя из этих принципов, а также опыта авторов, была предложена первоначальная схема соответствующего способа. Разработанные обобщенные алгоритмы для элементов схемы гипотетически обосновывают работоспособность всего способа и их применимость для задач информационной безопасности.

Продолжением исследования (после синтеза собственно инвариантных моделей и методов на основании предложенной схемы) должны стать детализация и практическая реализация алгоритмов оценивания и прогнозирования (дополненная вычислением показателей объекта [39]). Эксперименты с данными алгоритмами позволят оценить реальную работоспособность всего решения, а также его эффективность и применимость в «боевых условиях»; например, в сетевой [40-43] или социальной [44, 45] сферах.

Также, достаточно интересным с научной и практической точки зрения является применение способа оценивания и прогнозирования к области информационной безопасности, в том числе безопасности программного обеспечения. В этом случае под СлО понимается программа, обладающая множеством сложно взаимодействующих подпрограмм. Целью же применения способа будет определение метрик безопасности кода с позиции наличия или вероятности появления в нем программных ошибок [46, 47, 48].

Рецензент: *Шестаков Александр Викторович, доктор технических наук, старший научный сотрудник, проректор по научной работе Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, Россия.*

E-mail: vicerector.sc@sut.ru

Литература

1. Интеллектуальные сервисы защиты информации в критических инфраструктурах / И.В. Котенко, И.Б. Саенко, А.А. Чечулин [и др.]; под общей ред. И.В. Котенко, И.Б. Саенко. - СПб.: БХВ-Петербург, 2019. - 400 с. ISBN 978-5-9775-3968-5.
2. Десницкий В.А., Чечулин А.А., Котенко И.В., Левшун Д.С., Коломеец М.В. Комбинированная методика проектирования защищенных встроенных устройств на примере системы охраны периметра // Труды СПИИРАН. 2016. № 5 (48). С. 5-31.
3. Izrailov K., Chechulin A., Vitkova L. Threats Classification Method for the Transport Infrastructure of a Smart City // The proceedings of 14th International Conference on Application of Information and Communication Technologies (Tashkent, Uzbekistan, 7-9 October 2020). IEEE, 2020. P. 1-6.
4. Buinevich M., Izrailov K., Vladyko A. Metric of vulnerability at the base of the life cycle of software representations // The proceedings of 20th International Conference on Advanced Communication Technology (Chuncheon, South Korea, 2018). IEEE, 2018. PP. 1-8.
5. Васильев В.А., Добрынина Н.В. Информационная система оценки состояния сложного объекта // Фундаментальные проблемы радиоэлектронного приборостроения. 2016. Т. 16. № 4. С. 108-111.
6. Катасёва Д.В. Нейронечеткая модель и программный комплекс формирования баз знаний для оценки состояния объектов // Прикаспийский журнал: управление и высокие технологии. 2022. № 1 (57). С. 65-76.
7. Катасёв А.С. Нейронечеткая модель и программный комплекс автоматизации формирования нечетких правил для оценки состояния объектов // Автоматизация процессов управления. 2019. № 1 (55). С. 21-29.

8. Катасёв А.С. Нейронечеткая модель формирования нечетких правил для оценки состояния объектов в условиях неопределенности // Компьютерные исследования и моделирование. 2019. Т. 11. № 3. С. 477-492.
9. Калинчик И.В. Оценка и прогнозирование состояния систем электропотребления промышленных объектов // Енергетика: економіка, технології, екологія. 2013. № S. С. 41-46. eLIBRARY ID: 34464989
10. Назаров А.Н., Назаров М.А., Пантюхин Д.В., Сычев А.К., Покрова С.В. Автоматизация процедур мониторинга в Web-пространстве на основе нейро-нечёткого формализма // T-Comm: Телекоммуникации и транспорт. 2015. Т. 9. № 8. С. 26-33.
11. Акимов А.А., Мустафина С.И. Применение семантических сверточных нейронный сетей для детекции трещин дорожного покрытия // материалы международной научной конференции: Уфимская осенняя математическая школа - 2021 (Уфа, 06–09 октября 2021 года).2021. С. 128-131.
12. Сорокин А.А. Идентификация состояния сложного объекта на основе анализа сигнатуры его состояния // Математические методы в технике и технологиях - ММТТ. 2020. Т. 12-2. С. 30-35.
13. Аверин Г.В., Звягинцева А.В. Построение шкал для измерения состояний сложных объектов в многомерных пространствах // Вестник Донецкого национального университета. Серия Г: Технические науки. 2018. № 1. С. 13-23.
14. Kotenko I., Budko P., Vinogradenko A., Saenko I. An Approach for Intelligent Evaluation of the State of Complex Autonomous Objects Based on the Wavelet Analysis // Advancing Technology Industrialization Through Intelligent Software Methodologies, Tools and Techniques. H. Fujita and A. Selamat (Eds.). IOS Press, 2019. P.25-38.
15. Виноградeнко А.М. Интеллектуальное оценивание технического состояния сложных технических объектов // Техника средств связи. 2021. № 4 (156). С. 2-19.
16. Пучков А.Ю., Дли М.И., Лобанева Е.И. Применение глубоких нейронных сетей в моделях сложных технологических объектов // Известия Санкт-Петербургского государственного технологического института (технического университета). 2020. № 52 (78). С. 104-110.
17. Пучков А.Ю., Дли М.И., Лобанева Е.И. Модели сложных технологических объектов на основе сетей глубокого обучения // Математические методы в технике и технологиях - ММТТ. 2019. Т. 9. С. 8-10.
18. Федотов М.В., Грачев В.В. Предиктивная аналитика технического состояния систем тепловозов с использованием нейросетевых прогнозных моделей // Бюллетень результатов научных исследований. 2021. № 3. С. 102-114. DOI 10.20295/2223-9987-2021-3-102-114.
19. Федоров А.В., Шкодырев В.П., Барсуков Н.Д. Система ситуационного управления и контроля плохо формализуемых сценариев динамических сцен // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2018. Т. 11. № 3. С. 20-28.
20. Клячкин В.Н., Жуков Д.А. Прогнозирование состояния технического объекта с применением методов машинного обучения // Программные продукты и системы. 2019. № 2. С. 244-250.
21. Астахов С.А., Коновалов Д.В., Супонько К.Л., Щеголев Г.П. Прогнозирование технического состояния авиационных двигателей при их эксплуатации по состоянию // Авиационная промышленность. 2011. № 1. С. 11.
22. Булычев Д.И., Гречихин Н.С. Применение марковских цепей для прогнозирования состояния парка автомобилей в моделях с дискретным состоянием и непрерывным временем // Материалы Всероссийской научно-практической конференции: Математика: теоретические и прикладные исследования (Москва, 17 июня 2021 года). 2022. С. 43-47.
23. Вилисов В.Я. Применение марковских цепей для моделирования и прогнозирования развития пожара // Инженерный вестник Дона. 2021. № 3 (75). С. 159-169.
24. Дойникова Е.В., Котенко И.В. Оценивание защищенности и выбор контрмер для управления кибербезопасностью. СПб.: Изд-во «Наука», 2021. – 197 с. ISBN 978-5-907366-23-7.
25. Котенко И.В., Саенко И.Б. Создание новых систем мониторинга и управления кибербезопасностью // Вестник Российской академии наук. 2014. Т. 84. № 11. С. 993-1001.
26. Плохая Е. Е. Междисциплинарный характер трактовки понятия «информация» // Изоморфные и алломорфные признаки языковых систем: сборник статей по материалам IV ежегодной научно-практической конференции (Ставрополь, 12–19 апреля 2016 г.). 2016. С. 149-153.
27. Буйневич М.В., Израилов К.Е. Антропоморфический подход к описанию взаимодействия уязвимостей в программном коде. Часть 1. Типы взаимодействий // Защита информации. Инсайд. 2019. № 5 (89). С. 78-85.
28. Буйневич М.В., Израилов К.Е. Антропоморфический подход к описанию взаимодействия уязвимостей в программном коде. Часть 2. Метрика уязвимостей // Защита информации. Инсайд. 2019. № 6 (90). С. 61-65.
29. Васильева А.Ю., Израилов К.Е., Рамазанов А.И. Укрупненная методика оценки эффективности автоматизированных средств, восстанавливающих исходный код в целях поиска уязвимостей // Вестник ИНЖЭКОНа. Серия: Технические науки. 2013. № 8(67). С. 107-109.
30. Теслер Г.С. Системная методология прогнозирования: прогнозирование процессов естественной и искусственной природы // Математические машины и системы. 2004. № 1. С. 144-165.
31. Воронин Е.А., Захаров Д.Н. Построение самообучающихся графов динамических систем с сосредоточенными параметрами // Международный технико-экономический журнал. 2013. № 1. С. 67-69.
32. Безлепкин Е.А. Закономерности построения физических картин мира // Философия науки. 2016. № 4 (71). С. 67-82.
33. Буйневич М.В., Израилов К.Е., Покусов В.В., Ярошенко А.Ю. Основные принципы проектирования архитектуры современных систем защиты // Национальная безопасность и стратегическое планирование. 2020. № 3 (31). С. 51-58.
34. Максименко В.А. Аналитическое моделирование технической системы // Вестник Черниговского государственного технологического университета. Серия: Технические науки. 2011. № 2 (49). С. 10-14.
35. Львович И.Я., Преображенский А.П., Хромых А.А. Оценка средних характеристик рассеяния объектов // В мире научных открытий. 2013. № 2 (38). С. 188-200.
36. Богданов В.В., Петроневич В.В., Панченко И.Н., Куликов А.А., Лютов В.В., Бугров А.Ю., Манвелян В.С. Стенды для определения массы, координат центра масс и моментов инерции объектов // Авиакосмическое приборостроение. 2017. № 11. С. 28-39.
37. Аносов А.А., Беляев Р.В., Вилков В.А., Казанский А.С., Мансфельд А.Д., Шаракшанэ А.С. Определение динамики изменения температуры в модельном объекте методом акустотермографии // Акустический журнал. 2008. Т. 54. № 4. С. 540-545.

38. Садриддинов П.Б. Анализ температуры инициирования и максимальной температуры газа при фильтрационном горении газов // Вестник Таджикского национального университета. Серия естественных наук. 2019. № 4. С. 107-110.
39. Израилов К.Е. Система критериев оценки способов поиска уязвимостей и метрика понятности представления программного кода // Информатизация и связь. 2017. № 3. С. 111-118.
40. Kotenko I., Doynikova E. Security Assessment of Computer Networks based on Attack Graphs and Security Events // Lecture Notes in Computer Science. 2014. Vol.8407. P.462-471.
41. Браницкий А.А., Котенко И.В. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейро-нечетких классификаторов // Информационно-управляющие системы, 2015, № 4 (77), С. 69-77. DOI:10.15217. ISSN:1684-8853.2015.4.69.
42. Kotenko I., Chechulin A. Computer Attack Modeling and Security Evaluation based on Attack Graphs // Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS 2013. 2013. С. 614-619.
43. Лаврова Д.С., Попова Е.А., Штыркина А.А., Штеренберг С.И. Предупреждение dos-атак путем прогнозирования значений корреляционных параметров сетевого трафика // Проблемы информационной безопасности. Компьютерные системы. 2018. № 3. С. 70-77.
44. Shterenberg S.I., Poltavtseva M.A. A distributed intrusion detection system with protection from an internal intruder // Automatic Control and Computer Sciences. 2018. Т.52. №8. С. 945-953
45. Kotenko I., Saenko I., Chechulin A., Desnitsky V., Vitkova L., Pronoza A. Monitoring and counteraction to malicious influences in the information space of social networks // Lecture Notes in Computer Science, Vol.11186, Springer 2018. P. 159-167.
46. Израилов К.Е. Алгоритмизация машинного кода телекоммуникационных устройств как стратегическое средство обеспечения информационной безопасности // Национальная безопасность и стратегическое планирование. 2013. № 2 (2). С. 28-36.
47. Сахаров Д.В., Ковцур М.М., Бахтин Д.В. Модель защиты от эксплойтов и руткитов с последующим анализом и оценкой инцидентов // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 5. С. 22-31.
48. Марков А.С. Техническая защита информации. Курс лекций. М. АИСНТ. 2020.–234 С. ISBN 978-5-6045553-0-9

ASSESSMENT AND PREDICTION OF THE COMPLEX OBJECTS STATE: APPLICATIOIN FOR INFORMATION SECURITY

Izrailov K.E.[6], Buinevich M.V.[7], Kotenko I.V.[8], Desnitsky V.A.[9]

The goal of the study *is to create a method for estimating and predicting the state of objects with a non-trivial internal structure, multifunctional elements and complex relationships between them. An important feature of the goal is the independence of its solution from the area of operation of complex objects. The task of applying this approach in the field of information security is set.*

Research methods: *system analysis, analytical modeling methods, statistical methods and machine learning methods, development of program code for the implementation of assessment and forecasting algorithms.*

Result: *an ontological model of a generalized subject area is introduced that describes the main elements and their relationships. An analysis of the domestic scientific literature over the past few years and an analysis of the solutions existing in them are carried out, as well as their criteria-based comparison. The principles of constructing invariant methods of estimation and forecasting are developed. A scheme of a new method of estimation and forecasting is proposed. A description is given of generalized algorithms for the functioning of the assessment and prediction components, as well as their applicability for solving problems in the field of information security in the interests of countering network attacks.*

6 Konstantin E. Izrailov, Ph.D., Associate Professor of Dep. Secured Communication Systems of The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Senior Researcher of Laboratory of Computer Security Problems of St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint-Petersburg. ORCHID: https://orcid.org/0000-0002-9412-5693. Scopus Author ID: 56123238800. E-mail: konstantin.izrailov@mail.ru.

7 Mikhail V. Buinevich, Dr.Sc., Professor, Professor of Dep. Applied Mathematics and Information Technologies of Saint-Petersburg University of State Fire Service of EMERCOM of Russia, Saint-Petersburg. ORCHID: https://orcid.org/0000-0001-8146-0022. Scopus Author ID: 56122749800. E-mail: bmv1958@yandex.ru.

8 Igor V. Kotenko, Dr.Sc., Professor, Chief Scientist and Head of Laboratory of Computer Security Problems of St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint-Petersburg. ORCHID: https://orcid.org/0000-0001-6859-7120. Scopus Author ID: 15925268000. E-mail: ivkote@comsec.spb.ru.

9 Vasily A. Desnitsky, Ph.D., Senior Researcher of Laboratory of Computer Security Problems of St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint-Petersburg. ORCHID: https://orcid.org/0000-0002-3748-5414. Scopus Author ID: 36634098200. E-mail: desnitsky@comsec.spb.ru.

The scientific novelty *lies in a rather extensive review of works over the past ten years (mainly over the past five years) devoted to the evaluation and prediction of objects with a complex internal structure. The systematization of works aims not only at analyzing and criteria-based comparison of research results, but also at synthesizing solutions "tied" to a specific area of application. As a result, a method of estimation and forecasting is proposed, which, unlike similar ones, can work without taking into account the specifics of the subject area, and its use for information security is considered.*

Keywords: *information technology, ontological model, articles survey, criteria comparison, construction principles, hypothetical scheme, generalized algorithms, network security*

References

1. Intellektual'nyye servisy zashchity informatsii v kriticheskikh infrastrukturakh / I.V.Kotenko, I.B.Sayenko, A.A.Chechulin [i dr.]; pod obshchey red. I.V.Kotenko, I.B.Sayenko. SPb.: BKHV-Peterburg, 2019. 400 s. ISBN 978-5-9775-3968-5.
2. Desnitskiy V.A., Chechulin A.A., Kotenko I.V., Levshun D.S., Kolomeyets M.V. Kombinirovannaya metodika proyektirovaniya zashchishchennykh vstroyennykh ustroystv na primere sistemy okhrany perimetra // Trudy SPIIRAN. 2016. № 5 (48). S. 5-31.
3. Izrailov K., Chechulin A., Vitkova L. Threats Classification Method for the Transport Infrastructure of a Smart City // The proceedings of 14th International Conference on Application of Information and Communication Technologies (Tashkent, Uzbekistan, 7-9 October 2020). IEEE, 2020. PP. 1-6.
4. Buinevich M., Izrailov K., Vladyko A. Metric of vulnerability at the base of the life cycle of software representations // The proceedings of 20th International Conference on Advanced Communication Technology (Chuncheon, South Korea, 2018). IEEE, 2018. PP. 1-8.
5. Vasil'yev V.A., Dobrynina N.V. Informatsionnaya sistema otsenki sostoyaniya slozhnogo ob"yekta // Fundamental'nyye problemy radioelektronnogo priborostroyeniya. 2016. T. 16. № 4. S. 108-111.
6. Katasova D.V. Neyronechetkaya model' i programmnyy kompleks formirovaniya baz znaniy dlya otsenki sostoyaniya ob"yektov // Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii. 2022. № 1 (57). S. 65-76.
7. Katasov A.S. Neyronechetkaya model' i programmnyy kompleks avtomatizatsii formirovaniya nechetkikh pravil dlya otsenki sostoyaniya ob»yektov // Avtomatizatsiya protsessov upravleniya. 2019. № 1 (55). S. 21-29.
8. Katasov A.S. Neyronechetkaya model' formirovaniya nechetkikh pravil dlya otsenki sostoyaniya ob"yektov v usloviyakh neopredelennosti // Komp'yuternyye issledovaniya i modelirovaniye. 2019. T. 11. № 3. S. 477-492.
9. Kalinchik I.V. Ocenka i prognozirovanie sostojanija sistem jelektropotreblenija promyshlennyh ob"ektov // Energetika: ekonomika, tehnologiї, ekologija. 2013. № S. S. 41-46. eLIBRARY ID: 34464989
10. Nazarov A.N., Nazarov M.A., Pantyukhin D.V., Sychev A.K., Pokrova S.V. Avtomatizatsiya protsedur monitoringa v Web-prostranstve na osnove neyro-nechotkogo formalizma // T-Comm: Telekommunikatsii i transport. 2015. T. 9. № 8. S. 26-33.
11. Akimov A.A., Mustafina S.I. Primeneniye sematicheskikh svertochnykh neyronnyy setey dlya detektsii treshchin dorozhnogo pokrytiya // materialy mezhdunarodnoy nauchnoy konferentsii: Ufimskaya osennyaya matematicheskaya shkola - 2021 (Ufa, 06–09 oktyabrya 2021 goda).2021. S. 128-131.
12. Sorokin A.A. Identifikatsiya sostoyaniya slozhnogo ob"yekta na osnove analiza signatury yego sostoyaniya // Matematicheskiye metody v tekhnike i tekhnologiyakh - MMTT. 2020. T. 12-2. S. 30-35.
13. Averin G.V., Zvyagintseva A.V. Postroyeniye shkal dlya izmereniya sostoyaniy slozhnykh ob"yektov v mnogomernykh prostranstvakh // Vestnik Donetskogo natsional'nogo universiteta. Seriya G: Tekhnicheskiye nauki. 2018. № 1. S. 13-23.
14. Kotenko I., Budko P., Vinogradenko A., Saenko I. An Approach for Intelligent Evaluation of the State of Complex Autonomous Objects Based on the Wavelet Analysis // Advancing Technology Industrialization Through Intelligent Software Methodologies, Tools and Techniques. H. Fujita and A. Selamat (Eds.). IOS Press, 2019. P.25-38.
15. Vinogradenko A.M. Intellektual'noye otsenivaniye tekhnicheskogo sostoyaniya slozhnykh tekhnicheskikh ob"yektov // Tekhnika sredstv svyazi. 2021. № 4 (156). S. 2-19.
16. Puchkov A.YU., Dli M.I., Lobaneva Ye.I. Primeneniye glubokikh neyronnykh setey v modelyakh slozhnykh tekhnologicheskikh ob"yektov // Izvestiya Sankt-Peterburgskogo gosudarstvennogo tekhnologicheskogo instituta (tekhnicheskogo universiteta). 2020. № 52 (78). S. 104-110.
17. Puchkov A.YU., Dli M.I., Lobaneva Ye.I. Modeli slozhnykh tekhnologicheskikh ob"yektov na osnove setey glubokogo obucheniya // Matematicheskiye metody v tekhnike i tekhnologiyakh - MMTT. 2019. T. 9. S. 8-10.
18. Fedotov M.V., Grachev V.V. Prediktivnaya analitika tekhnicheskogo sostoyaniya sistem teplovozov s ispol'zovaniyem neyrosetevykh prognoznykh modeley // Byulleten' rezul'tatov nauchnykh issledovaniy. 2021. № 3. S. 102-114. DOI 10.20295/2223-9987-2021-3-102-114.
19. Fedorov A.V., Shkodyrev V.P., Barsukov N.D. Sistema situatsionnogo upravleniya i kontrolya plokho formalizuyemykh stsenariyev dinamicheskikh stsen // Nauchno-tekhnicheskiye vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo universiteta. Informatika. Telekommunikatsii. Upravleniye. 2018. T. 11. № 3. S. 20-28.
20. Klyachkin V.N., Zhukov D.A. Prognozirovaniye sostoyaniya tekhnicheskogo ob"yekta s primeneniyem metodov mashinnogo obucheniya // Programmnyye produkty i sistemy. 2019. № 2. S. 244-250.
21. Astakhov S.A., Konovalov D.V., Supon'ko K.L., Shchegolev G.P. Prognozirovaniye tekhnicheskogo sostoyaniya aviatsionnykh dvigateley pri ikh ekspluatatsii po sostoyaniyu // Aviatsionnaya promyshlennost'. 2011. № 1. S. 11.
22. Bulychev D.I., Grechikhin N.S. Primeneniye markovskikh tsepey dlya prognozirovaniya sostoyaniya parka avtomobiley v modelyakh s diskretnym sostoyaniyem i nepreryvnym vremenem // materialy Vserossiyskoy nauchno-prakticheskoy konferentsii: Matematika: teoreticheskiye i prikladnyye issledovaniya (Moskva, 17 iyunya 2021 goda). 2022. S. 43-47.
23. Vilisov V.YA. Primeneniye markovskikh tsepey dlya modelirovaniya i prognozirovaniya razvitiya pozhara // Inzhenernyy vestnik Dona. 2021. № 3 (75). S. 159-169.
24. Doynikova Ye.V., Kotenko I.V. Otsenivaniye zashchishchennosti i vybor kontrmer dlya upravleniya kiberbezopasnost'yu. SPb.: Izd-vo

«Nauka», 2021. – 197 s. ISBN 978-5-907366-23-7.
25. Kotenko I.V., Sayenko I.B. Sozdaniye novykh sistem monitoringa i upravleniya kiberbezopasnost'yu // Vestnik Rossiyskoy akademii nauk. 2014. T. 84. № 11. S. 993-1001.
26. Plokhaya Ye. Ye. Mezhdistsiplinarnyy kharakter traktovki ponyatiya «informatsiya» // Izomorfnyye i allomorfnyye priznaki yazykovykh sistem: sbornik statey po materialam IV yezhegodnoy nauchno-prakticheskoy konferentsii (Stavropol', 12–19 aprelya 2016 g.). 2016. S. 149-153.
27. Buynevich M.V., Izrailov K.Ye. Antropomorficheskiy podkhod k opisaniyu vzaimodeystviya uyazvimostey v programmnom kode. Chast' 1. Tipy vzaimodeystviy // Zashchita informatsii. Insayd. 2019. № 5 (89). S. 78-85.
28. Buynevich M.V., Izrailov K.Ye. Antropomorficheskiy podkhod k opisaniyu vzaimodeystviya uyazvimostey v programmnom kode. Chast' 2. Metrika uyazvimostey // Zashchita informatsii. Insayd. 2019. № 6 (90). S. 61-65.
29. Vasil'yeva A.YU., Izrailov K.Ye., Ramazanov A.I. Ukrupnennaya metodika otsenki effektivnosti avtomatizirovannykh sredstv, vosstanavlivayushchikh iskhodnyy kod v tselyakh poiska uyazvimostey // Vestnik INZHEKONa. Seriya: Tekhnicheskiye nauki. 2013. № 8(67). S. 107-109.
30. Tesler G.S. Sistemnaya metodologiya prognozirovaniya: prognozirovaniye protsessov yestestvennoy i iskusstvennoy prirody // Matematicheskiye mashiny i sistemy. 2004. № 1. S. 144-165.
31. Voronin Ye.A., Zakharov D.N. Postroyeniye samoobuchayushchikhsya grafov dinamicheskikh sistem s sosredotochennymi parametrami // Mezhdunarodnyy tekhniko-ekonomicheskiy zhurnal. 2013. № 1. S. 67-69.
32. Bezlepkin Ye.A. Zakonomernosti postroyeniya fizicheskikh kartin mira // Filosofiya nauki. 2016. № 4 (71). S. 67-82.
33. Buynevich M.V., Izrailov K.Ye., Pokusov V.V., Yaroshenko A.YU. Osnovnyye printsipy proyektirovaniya arkhitektury sovremennykh sistem zashchity // Natsional'naya bezopasnost' i strategicheskoye planirovaniye. 2020. № 3 (31). S. 51-58.
34. Maksimenko V.A. Analiticheskoye modelirovaniye tekhnicheskoy sistemy // Vestnik Chernigovskogo gosudarstvennogo tekhnologicheskogo universiteta. Seriya: Tekhnicheskiye nauki. 2011. № 2 (49). S. 10-14.
35. L'vovich I.YA., Preobrazhenskiy A.P., Khromykh A.A. Otsenka srednikh kharakteristik rasseyaniya ob"yektov // V mire nauchnykh otkrytiy. 2013. № 2 (38). S. 188-200.
36. Bogdanov V.V., Petronevich V.V., Panchenko I.N., Kulikov A.A., Lyutov V.V., Bugrov A.YU., Manvelyan V.S. Stendy dlya opredeleniya massy, koordinat tsentra mass i momentov inertsii ob"yektov // Aviakosmicheskoye priborostroyeniye. 2017. № 11. S. 28-39.
37. Anosov A.A., Belyayev R.V., Vilkov V.A., Kazanskiy A.S., Mansfel'd A.D., Sharakshane A.S. Opredeleniye dinamiki izmeneniya temperatury v model'nom ob"yekte metodom akustotermografii // Akusticheskiy zhurnal. 2008. T. 54. № 4. S. 540-545.
38. Sadriddinov P.B. Analiz temperatury initsiirovaniya i maksimal'noy temperatury gaza pri fil'tratsionnom gorenii gazov // Vestnik Tadzhikskogo natsional'nogo universiteta. Seriya yestestvennykh nauk. 2019. № 4. S. 107-110.
39. Izrailov K.Ye. Sistema kriteriyev otsenki sposobov poiska uyazvimostey i metrika ponyatnosti predstavleniya programmnogo koda // Informatizatsiya i svyaz'. 2017. № 3. S. 111-118.
40. Kotenko I., Doynikova E. Security Assessment of Computer Networks based on Attack Graphs and Security Events // Lecture Notes in Computer Science. 2014. Vol 8407. P 462-471.
41. Branitskiy A.A., Kotenko I.V. Obnaruzheniye setevykh atak na osnove kompleksirovaniya neyronnykh, immunnykh i neyro-nechetkikh klassifikatorov // Informatsionno-upravlyayushchiye sistemy, 2015, № 4 (77), S. 69-77. 'DOI:10.15217. ISSN:1684-8853.2015.4.69.
42. Kotenko I., Chechulin A. Computer Attack Modeling and Security Evaluation based on Attack Graphs // Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS 2013. 2013. S. 614-619.
43. Lavrova D.S., Popova Ye.A., Shtyrkina A.A., Shterenberg S.I. Preduprezhdeniye dos-atak putem prognozirovaniya znacheniy korrelyatsionnykh parametrov setevogo trafika // Problemy informatsionnoy bezopasnosti. Komp'yuternyye sistemy. 2018. № 3. S. 70-77.
44. Shterenberg S.I., Poltavtseva M.A. A distributed intrusion detection system with protection from an internal intruder // Automatic Control and Computer Sciences. 2018. T. 52. №8. S. 945-953
45. Kotenko I., Saenko I., Chechulin A., Desnitsky V., Vitkova L., Pronoza A. Monitoring and counteraction to malicious influences in the information space of social networks // Lecture Notes in Computer Science, Vol 11186, Springer 2018. P. 159-167.
46. Izrailov K.Ye. Algoritmizatsiya mashinnogo koda telekommunikatsionnykh ustroystv kak strategicheskoye sredstvo obespecheniya informatsionnoy bezopasnosti // Natsional'naya bezopasnost' i strategicheskoye planirovaniye. 2013. № 2 (2). S. 28-36.
47. Sakharov D.V., Kovtsur M.M., Bakhtin D.V., Model' zashchity ot eksploytov i rutkitov s posleduyushchim analizom i otsenkoy intsidentov // Naukoyemkiye tekhnologii v kosmicheskikh issledovaniyakh Zemli. 2019. T. 11. № 5. S. 22-31.
48. Markov A.S. Tehnicheskaja zashhita informacii. Kurs lekcij. M. AISNT. 2020.–234 S. ISBN 978-5-6045553-0-9