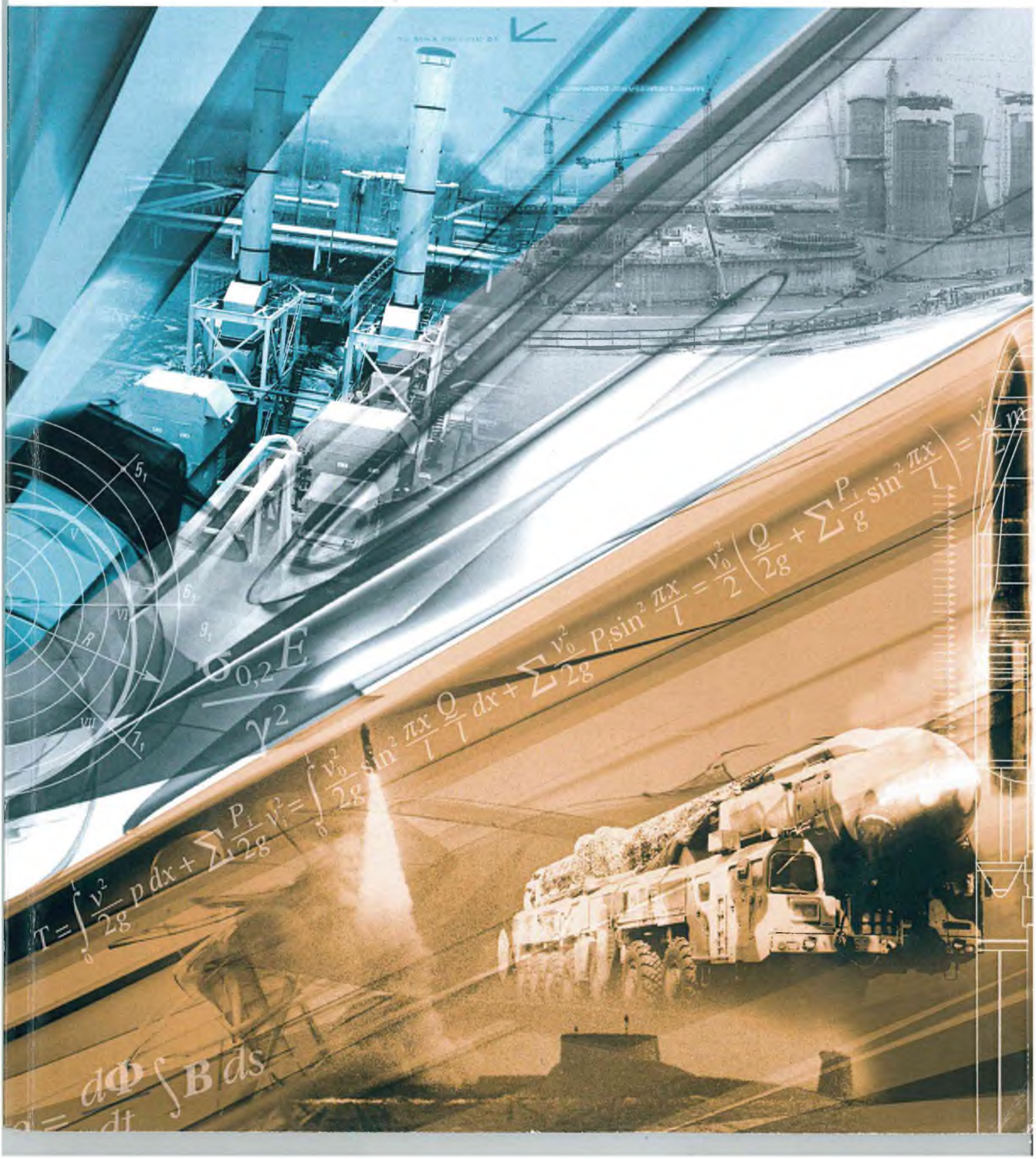
ВОЕННО-ИНЖЕНЕРНАЯ КОРПОРАЦИЯ
РОССИЙСКАЯ ИНЖЕНЕРНАЯ АКАДЕМИЯ
Секция «Инженерные проблемы стабильности и конверсии»

ISSN 1680-2780

Двойные технологии

№ 3
2019



ДВОЙНЫЕ ТЕХНОЛОГИИ №3 (88) 2019

РОССИЙСКАЯ ИНЖЕНЕРНАЯ АКАДЕМИЯ
СЕКЦИЯ «ИНЖЕНЕРНЫЕ ПРОБЛЕМЫ СТАБИЛЬНОСТИ И КОНВЕРСИИ»

АКЦИОНЕРНОЕ ОБЩЕСТВО
«ВОЕННО–ИНЖЕНЕРНАЯ КОРПОРАЦИЯ»

Издается с сентября 1997 г.
Свидетельство о регистрации
ПИ №77-3609 от 05.06.2000 г.
ISSN 1680-2780

Выходит 4 раза в год

Журнал включен
в «Перечень ведущих периодических изданий» ВАК
и систему РИНЦ

Научно-технический журнал
Наукоемкие технологии, проекты двойного использования комплексов вооружений, техногенная и другие виды безопасностей эксплуатации военных систем, экологический мониторинг.

Группы специальностей: авиационная и ракетно-космическая техника (05.07.00); радиотехника и связь (05.12.00); информатика, вычислительная техника и управление (05.13.00) (технические, физико-математические науки).

СОДЕРЖАНИЕ

УДК 004.056

© Глухов А.П., Бирюков Д.Н., Василенко В.В., Корниенко А.А., Сидак А.А.

© Glukhov A., Biryukov D., Vasilenko V., Kornienko A., Sidak A.

МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ УПРЕЖДАЮЩЕГО УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

METHODOLOGICAL ASPECTS OF PROACTIVE MANAGEMENT OF RAILROAD TRANSPORT INFORMATION SECURITY

Аннотация. *Рассмотрены новые риски информационной безопасности при реализации Концепции цифровой железной дороги. С целью снижения рисков предложено развитие существующей системы управления информационной безопасностью, направленное на интеллектуализацию системы и наделение ее способностью по предотвращению компьютерных атак, априорно неизвестных на момент создания системы защиты информации, но смоделированных интеллектуальной системой.*

Рассмотрен подход к определению результативности упреждающего управления с точки зрения оперативности решения задач противодействия. Показана роль структуризации автоматизированных информационных систем и реализации эшелонированной системы защиты информации для повышения эффективности процессов ситуационного упреждающего управления информационной безопасностью.

Abstract. *Considered new information security risks in the implementation of the concept of digital railroad. In order to reduce risks, the development of the existing information security management system has been proposed, aimed at intellectualizing the system and endowing it with the ability to prevent computer attacks that are a priori unknown at the time of creating the information protection system, but modeled by an intelligent system.*

The approach to determining the effectiveness of proactive management from the point of view of efficiency of solving the tasks of counteraction is considered. The role of the structuring of automated information systems and the implementation of the layered information protection system to improve the efficiency of the processes of situational proactive information security management is shown.

Ключевые слова. *Упреждающее управление, информационная безопасность, железнодорожный транспорт, интеллектуальная система управления, структуризация, эшелонированная защита, ложный компонент, мониторинг, инцидент.*

Key words. *Proactive management, information security, railroad transport, intelligent control system, structuring, defense in depth, false component, monitoring, incident.*

В настоящее время одним из стратегических направлений инновационного развития железнодорожного транспорта (ЖТ) является создание единого цифрового пространства и интеллектуализация ЖТ [1, 2, 3].

Интеллектуализация ЖТ определяет возрастающую роль факторов информационной безопасности (ИБ) в управлении ЖТ, в том числе при решении проблем безопасности движения, пассажирских и грузовых перевозок.

Эти факторы будут решающими при организации высокоскоростного движения и построении интеллектуальных центров и систем ситуационного управления, особенно с учетом исходящих из киберпространства угроз ИБ и потенциальной подверженности информационной инфраструктуры (ИИ) ЖТ компьютерным атакам (КА).

Интеллектуальное управление железнодорожным транспортом положено в основу концепции создания цифровой железной дороги (ЦЖД) [3].

Новые технологии ЦЖД направлены на повышение эффективности деятельности железнодорожной отрасли во всех функциональных областях. В то же время планируемые к применению технологии «интернет-вещей», «большие данные», «облачные вычисления», «мобильные и социальные коммуникации» несут новые риски ИБ ИИ ЖТ (см. рис. 1).

Глухов Александр Петрович *– доктор технических наук, доцент кафедры «Информатика и информационная безопасность», ФГБОУ ВО «Петербургский государственный университет путей сообщения императора Александра I», e-mail: gala606@rambler.ru;*

Бирюков Денис Николаевич *– доктор технических наук, доцент, заведующий кафедрой, Военно-космическая академия имени А.Ф. Можайского, e-mail: Biryukov.D.N@yandex.ru;*

Василенко Владимир Васильевич *– доктор технических наук, профессор, заместитель председателя, ООО «Центр безопасности информации», e-mail: v.vasilenko@cbi-info.ru;*

Корниенко Анатолий Адамович *– доктор технических наук, профессор, заведующий кафедрой «Информатика и информационная безопасность», ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I», e-mail: kaa.pgups@yandex.ru;*

Сидак Алексей Александрович *– кандидат технических наук, старший научный сотрудник, заместитель председателя, ООО «Центр безопасности информации», e-mail: sidak@cbi-info.ru.*

Glukhov Alexander *– doctor of technical sciences, docent of department, PGUPS, e-mail: gala606@rambler.ru.*

Biryukov Denis *– doctor of technical science, docent, head of department, VKA, e-mail: Biryukov.D.N@yandex.ru.*

Vasilenko Vladimir *– doctor of technical science, professor, deputy chairman, Information Security Center, e-mail: v.vasilenko@cbi-info.ru;*

Kornienko Anatoly *– doctor of technical sciences, professor, head of department, PGUPS, kaa.pgups@yandex.ru;*

Sidak Aleksey *– candidate of technical science, senior researcher, deputy chairman, Information Security Center, e-mail: sidak@cbi-info.ru.*

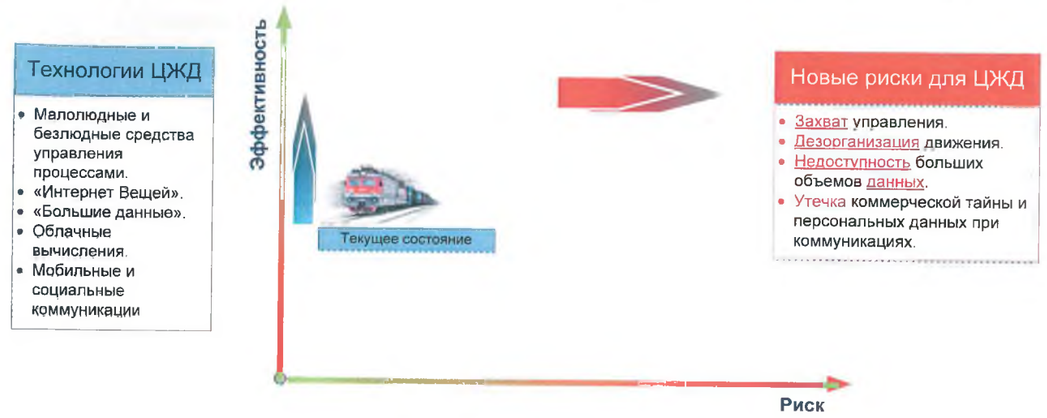


Рис. 1. Технологии и новые риски ИБ ИИ ЖТ

При этом вопросы анализа и управления рисками ИБ ИИ ЖТ являются ключевыми и должны рассматриваться, с одной стороны, применительно к функциональным областям, а с другой стороны, в связи с применяемыми классами автоматизированных решений и конкретных технологий (см. рис. 2).

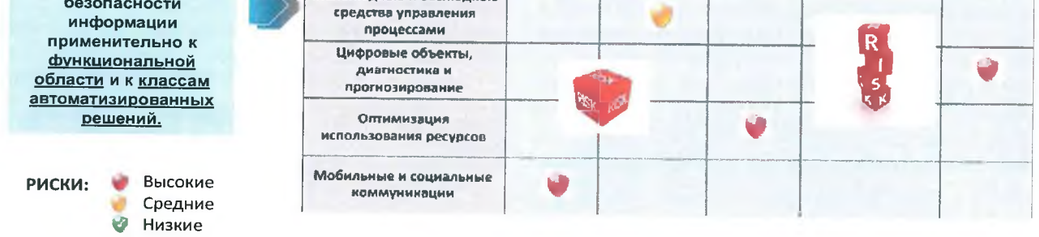


Рис. 2. Риски ИБ ИИ ЖТ применительно к функциональным областям и классам автоматизированных решений

Управление ИБ ИИ ЖТ, под которым понимается целенаправленное изменение состояния информационных активов с целью минимизации возможного ущерба (обеспечения приемлемого уровня) в интересах достижения бизнес-целей предприятий ЖТ, может быть корректирующим (корректирующие действия, следящее управление) и проактивным или упреждающим (превентивные действия, прогнозное управление ИБ).

Основной целью обеспечения ИБ ИИ ЖТ является снижение рисков ИБ, действующих в отношении информационных ресурсов, и в конечном счете предотвращение или минимизация ущерба от возможных инцидентов ИБ [4].

Сокращение инцидентов ИБ путём эффективного использования современных средств защиты сетей, компьютерных систем, программного обеспечения (ПО) может быть достигнуто за счет принятия превентивных мер ИБ (предотвращение проблем до наступления инцидента ИБ).

В настоящее время процессы управления рисками и инцидентами ИБ в существующих системах управления ИБ (СУИБ) ЖТ в основном ориентированы на корректирующие действия и реагирование, как правило, на свершившееся нежелательное событие, связанное с нарушением ИБ [5]. В то же время риск-ориентированное планирование и оперативное управление инцидентами ИБ должны быть тесно взаимосвязанными процессами риск-ориентированного управления ИБ ИИ ЖТ, в значительной мере направленными на превентивные действия и упреждающее управление ИБ.

При этом перспективным видится такой подход, при котором средства обеспечения ИБ ИИ ЖТ были бы “интеллектуально” способны предотвращать и типы воздействий, которые априорно не известны на момент создания системы защиты информации (СЗИ), но могут быть смоделированы с применением интеллектуальных систем [6].

В связи с этим для формирования сценариев упреждающего поведения в ходе риск-ориентированного управления ИБ ИИ ЖТ предлагается применять интеллектуальные системы управления ИБ (ИСУИБ) [7], способные в процессе функционирования формировать модель окружающей киберсреды и синтезировать программу действий в соответствии с целями, состоя-

щими в поддержании требуемого уровня защищённости от возможных КА.

Способность ИСУИБ к предотвращению атакующих воздействий на защищаемые ресурсы должна опираться на три базовые способности: обнаружение, предупреждение и пресечение. При этом в рамках обнаружения и предупреждения должно осуществляться прогнозирование развития наблюдаемых ситуаций, идентификация возможных задач, требующих решения, и построение моделей действий, обеспечивающих предотвращение возможных негативных последствий.

Для того чтобы перспективная ИСУИБ ЖТ была способной порождать сценарии упреждающего поведения в информационном конфликте, она должна относиться к классу самоорганизующихся систем, а для этого она должна быть многоагентной, и её агенты должны унифицировано взаимодействовать [8, 9], а также способной порождать результативные стратегии поведения под влиянием внешней среды.

Реализация принципов, методов, моделей и алгоритмов ИСУИБ может осуществляться через построение и функционирование системы интеллектуальных сервисов ЗИ как нового и важнейшего компонента СЗИ в ИИ ЖТ, позволяющую осуществлять интегральную оценку состояния ИИ, управление ИБ и адаптацию политик ИБ и компонентов СЗИ [6, 10].

Одним из важнейших аспектов ситуационного управления ИБ ИИ ЖТ является управление инцидентами ИБ [5, 9]. Управление сложными информационными системами транспортного назначения требует постоянного мониторинга и анализа событий ИБ. Для предотвращения либо оперативной минимизации последствий инцидентов ИБ нужен сбор, анализ информации, моделирование и оценка решений, координация действий в режиме реального времени.

В развитие подходов обеспечения ИБ ИИ ЖТ [11] предлагается наделить СУИБ ЖТ принципиально новым свойством, позволяющим им предвидеть развитие событий, явлений, результатов действий (антиципация) [8].

Под антиципирующими ИСУИБ ЖТ предлагается понимать такие системы, которые способны принимать решения и действовать с определенным упреждением в отношении ожидаемых событий, направленных на нарушение политики ИБ ИИ ЖТ, на основе:

- информации, получаемой из внешней среды через совокупность сенсоров (агентов);
- информации о прошлом опыте;
- сопоставления информации, полученной от сенсоров, с имеющейся информацией;
- выдвижения гипотезы о возможных отдаленных событиях;
- порождения стратегии целенаправленного поведения системы;
- поддержания требуемого уровня ИБ.

Последовательное выполнение перечисленных операций может быть представлено в виде типового сценария поведения в конфликте.

Функционирование интеллектуальной СУИБ ЖТ предлагается рассмотреть через многомодельное представление процессов взаимодействия конфликтующих сторон и описать на нескольких стратах [10] (см. рис. 3):

- страта 1 – искомая способность ИСУИБ: предотвращение КА на ИИ ЖТ;
- страта 2 – первичная декомпозиция способности предотвращения КА;
- страта 3 – рассмотрение способности предотвращения КА с точки зрения свойства антиципации;
- страта 4 – киберинтерпретация антиципации (цикл принятия решений ИСУИБ по предотвращению КА).

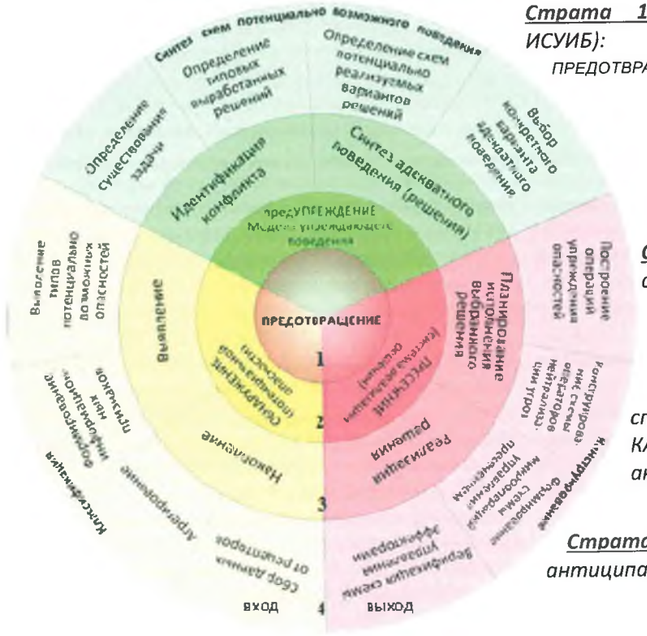


Рис. 3. Представление процессов функционирования ИСУИБ ЖТ с упреждающим поведением

Страта 1 *(ядро – искомая способность ИСУИБ):*

ПРЕДОТВРАЩЕНИЕ КОМПЬЮТЕРНЫХ АТАК НА ИИ ЖТ

Страта 2 *(первичная декомпозиция способности предотвращения КА)*

Страта 3 *(рассмотрение способности предотвращения КА с точки зрения свойства антиципации)*

Страта 4 *(киберинтерпретация антиципации)*

Отличительной характеристикой ИСУИБ ЖТ от систем рефлекторного поведения [12] является наличие в ней (кроме модуля восприятия "В" и модуля реакции "Р") модуля прогнозирования "П", функционирование которого основано на обработке соответствующей семантической информации (см. рис. 4).

Рис.4. Обобщённая схема интеллектуальной СУИБ ЖТ

Интеллектуальную СУИБ ЖТ предлагается рассматривать как систему, способную к самообучению, которая может осуществлять операции над смыслами, манипулируя накопленными знаниями для извлечения потенциально возможных решений по ИБ [13,14].

Обучение ИСУИБ можно проводить на специально создаваемых в ИИ ложных компонентах информационных технологий, предназначенных для перенаправления на эти компоненты нарушителя при реализации последним КА. При этом могут быть обнаружены новые актуальные угрозы ИБ [15], а также появится возможность экспериментирования в борьбе с ними, не опасаясь ошибок первого и второго рода.

В целях обучения ИСУИБ ИИ ЖТ могут использоваться результаты функционирования комплексных систем мониторинга и реагирования на инциденты ИБ типа NEURODAT [9].

В целом проблему предотвращения риска разнородно-массовых деструктивных воздействий на ИИ ЖТ предлагается свести к проблеме синтеза системы знаний для порождения сценариев упреждающего поведения. Чем более интеллектуальной будет СУИБ, тем эффективнее она сможет спрогнозировать возможные и наиболее опасные реализации угроз ИБ и выработать спецификации их упреждающей нейтрализации.

Для реализации ситуационного упреждающего управления ИБ в ИИ ЖТ необходимо обеспечить:

- представление знаний об источниках угроз ИБ и процессах ситуационного управления ИБ;
- получение новых знаний о многоэтапных деструктивных воздействиях на объекты ИИ ЖТ и о возможностях их нейтрализации;
- формирование спецификаций программ ситуационного управления инцидентами ИБ.

Для описания знаний об источниках угроз ИБ и возможных процессах ситуационного управления инцидентами ИБ предлагается использовать три класса концептов: «объекты», «свойства» и «действия». Также предлагается использовать ограниченный перечень ролей, которые могут применяться для задания отношений между концептами указанных типов.

Новые знания о многоэтапных деструктивных воздействиях на объекты ИИ ЖТ могут быть получены как из общедоступных источников (база данных угроз ФСТЭК России, базы компьютерных атак ATT&CK, Common Attack Pattern Enumeration and Classification и другие), так и полученных на основе результатов анализа угроз ИБ для автоматизированных информационных систем, подобных рассматриваемым в ИИ ЖТ [15].

Очевидно, что пополнять базу знаний ИСУИБ ЖТ можно либо информацией, которая предоставляется экспертами, либо информацией (знаниями), порожденной самой ИСУИБ, сокращая тем самым время пополнения базы знаний, а следовательно, и время выработки решений по обеспечению безопасности ИИ ЖТ. Например, в ситуации, когда ИСУИБ ЖТ последовательно формирует базу знаний о реализациях КА, она впоследствии сможет строить модели соответствующих процессов с прогнозированием упреждающего поведения.

В дальнейшем для формирования спецификаций программ ситуационного упреждающего управления ИБ ИИ ЖТ могут применяться возможности аппарата аппликативно-комбинаторных вычислений, позволяющего формировать из базовых функций (действий, процедур, программ и т.п.) и функциональных форм (которые в свою очередь задаются исходя из семантики предметной области) более сложные функциональные конструкции спецификаций [8, 13].

Применение аппликативного подхода к описанию потенциально реализуемых процессов способствует реализации в ИСУИБ ЖТ процедуры направленного комбинирования, основанной на применении ограниченного перечня доступных функциональных форм $[[O_1 \to P_1] \to A_1] \to [O_2 \to P_2]$, то есть «объект O_1, обладающий свойством P_1, способен осуществить воздействие A_1 на объект O_2, поскольку последний обладает свойством P_2»), что позволит уменьшить число порождаемых некорректных спецификаций ещё на этапе их формирования.

В целях реализации процедуры направленной обработки данных для формирования спецификаций упреждающего поведения разработана модель ассоциативной ресурсной сети (АРС) [6,13,14], которая позволяет в результате накопления опыта ИСУИБ ЖТ изменять доступность знаний, представленных в её памяти (см. рис. 5). Разработанная модель распространения ассоциативного сигнала по АРС позволила описать процесс «забывания» редко используемых и ложных знаний путём снижения уровня их доступности.

Упреждающее поведение ИСУИБ предлагается свести к синтезу такого сценария поведения, в ходе которого она способна изменить ход запланированного к реализации атакующей стороной процесса, приводящего к негативным для защищаемой ИИ ЖТ последствиям [16, 12]. Таким образом может быть функционально расширена стадия сдерживания инцидента ИБ, включающая [5]:

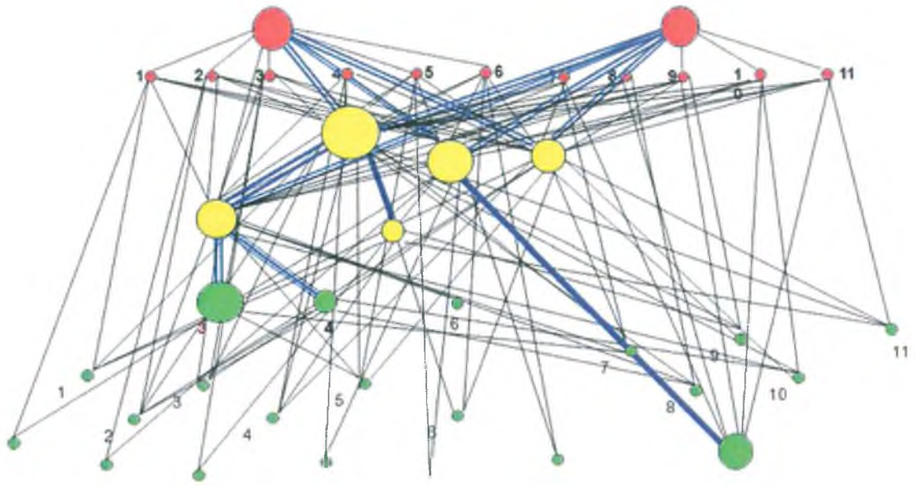


Рис. 5. Графическое представление ассоциативной ресурсной сети

• локализацию и отключение объекта, связанного с инцидентом ИБ;

• переконфигурацию сетевого оборудования для блокирования сетевых адресов или портов;

• блокировку доступа скомпрометированных компонентов ИИ ЖТ к информационно-телекоммуникационной сети;

• полную блокировку сетевого трафика с сетевых адресов компонентов ИИ ЖТ;

• блокировку скомпрометированной учетной записи;

• мониторинг и блокировку несанкционированных каналов связи;

• другие действия по сдерживанию инцидента ИБ.

Рассмотрим пример: пусть к моменту времени ИСУИБ ЖТ накопила данные, необходимые и достаточные для построения моделей возможно реализуемых процессов, схематично представленных в виде различных траекторий на рис. 6.

При этом различные процессы могут быть потенциально завершены с различными результатами. Некоторые результаты приемлемы для защищаемой ИИ ЖТ, а некоторые нет (см. оценки от “-3” до “+2” на рис.6). Важным моментом является то, что ИСУИБ может на отдельных этапах потенциально реализуемых процессов повлиять на их ход (см. узлы “B”,“D”,“E”,“F”,“I”). Пусть наиболее вероятен процесс “A-M”, который завершается с наихудшим исходом (“-3”), тогда, если ИСУИБ ЖТ для моделирования процессов противоборства и выбора приемлемого варианта упреждающего поведения требуется t_3–t_0 времени, то она не сможет предложить ни одного приемлемого решения, если же системе потребуется менее чем t_1–t_0 времени, то она сможет предложить на выбор целый ряд альтернатив.

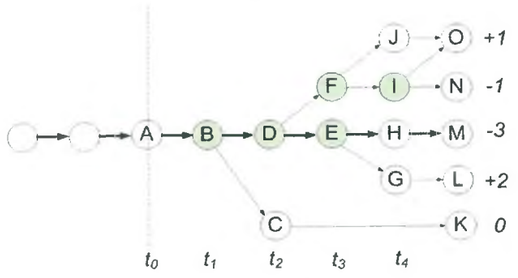


Рис. 6. Траектории возможно реализуемых процессов

Таким образом, в результативность ИСУИБ важнейший вклад вносит оперативность ее реакции на деструктивные воздействия.

С целью определения возможного подхода к определению результативности упреждающего управления, с точки зрения оперативности решения задач противодействия КА, целесообразно рассматривать ИСУИБ как сложную систему управления с непрерывным временем и с завершающим (поглощающим) состоянием, в которой информационные процессы не имеют конфликтов из-за ресурсов, так как все их ресурсы монопольно используются для решения основной функциональной задачи ИСУИБ ЖТ. Основные риски ИСУИБ ЖТ могут быть связаны с несвоевременным завершением процессов в цикле управления, а также с наиболее критическим сценарием применения ИСУИБ, например, с режимом оперативной корректировки функциональных задач [17].

В качестве одной из наиболее полных характеристик устойчивости ИСУИБ ЖТ можно рассматривать функцию распределения времени завершения цикла управления, в том числе и с учетом возможных информационных воздействий на ИСУИБ. Поглощающее состояние ИСУИБ определяется наступлением события завершения решения функциональных задач ИСУИБ. Функция распределения времени завершения цикла управления может быть экспериментальной, может быть в ряде случаев получена аналитически. Путем ее использования можно решать как задачи анализа, так и задачи синтеза процессов ситуационного упреждающего управления ИБ для улучшения их оперативных характеристик и снижения рисков не выполнения ИСУИБ ЖТ своих функциональных задач.

В целях уменьшения размерности задач распознавания деструктивных воздействий и синтеза процессов ситуационного упреждающего управления ИБ автоматизированные информационные системы в составе ИИ ЖТ целесообразно соответствующим образом структурировать [18]: выделить сегменты, локализовать в этих сегментах защищаемые виды информации, сформировать [19] и реализовать функциональные требования безопасности [20] по созданию эшелонированной системы защиты информации (СЗИ) [18], включив в состав средств защиты информации на соответствующих уровнях СЗИ средства реализации процессов ситуационного упреждающего управления ИБ.

Заключение. Планируемые к применению в ИИ ЖТ технологии «интернет-вещей», «большие данные», «облачные вычисления», «мобильные и социальные коммуникации» и др. несут новые риски с точки зрения обеспечения безопасности информации. При этом вопросы анализа и управления рисками ИБ ИИ ЖТ являются ключевыми и должны рассматриваться, с одной стороны, применительно к функциональным областям, а с другой стороны, в связи с применяемыми классами автоматизированных решений и конкретных технологий ИИ ЖТ.

Для обеспечения необходимого уровня ИБ ИИ ЖТ необходимо создание полномасштабной многоуровневой ИСУИБ ЖТ от КА, эффективность которой во многом будет определена интеллектуальной системой управления, основанной на риск-ориентированном, ситуационном и упреждающем подходах.

Для повышения результативности противодействия атакующим воздействиям при обеспечении ИБ ИИ ЖТ в условиях априорной неопределенности разнородно-массовых воздействий представляется необходимым синтезировать систему знаний на основе их многомодельного представления, способную порождать сценарии управления ИБ объектов ИИ ЖТ, что предполагает построение языков, грамматик и семантик описания и представления знаний и механизмов манипулирования ими.

На результативность процесса порождения сценариев упреждающего поведения в общем случае оказывают влияние объем имеющихся у ИСУИБ ЖТ знаний, поступающие на вход(ы) данные, язык представления знаний и правила порождения новых знаний из имеющихся, а также время выработки решений по упреждению в конфликте.

Методы интеллектуализации управления ИБ предлагается интегрировать с централизованно применяемыми в железнодорожной отрасли системами мониторинга и управления инцидентами ИБ [5, 9].

Литература

1 Гапанович В.А., Розенберг И.Н. Основные направления развития интеллектуального железнодорожного транспорта // Железнодорожный транспорт. – 2011. – № 4. – С. 5-11.

2. Ковалев В.И., Корниенко А.А. Интеллектуальный поезд и «умные» железные дороги: международный и отечественный опыт, состояние, проблемные вопросы // Материалы I Международной научно–практической конференции «ИнтеллектТранс–2011» – СПб.: ПГУПС. – 2011. – С. 24-31.

3. Розенберг Е.Н. Цифровая железная дорога – ближайшее будущее // Автоматика, связь, информатика. – 2016. – № 10. – С. 4-7.

4. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч. / С.Е. Ададуров, А.П. Глухов, А.А. Корниенко; под ред. А. А. Корниенко. – М.: ФГБОУ «Учебно–методический центр по образованию на железнодорожном транспорте». 2014. – ч. 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте. – 440 с.

5. Ададуров С.Е., Глухов А.П., Сидак А.А., Рулёв А.С., Петрейко А.В. Реагирование на инциденты информационной безопасности в микропроцессорных системах железнодорожной автоматики и телемеханики // Двойные технологии. – 2018. – № 2. – С. 76-81.

6. Глухов А.П. Многомодельное представление знаний и модель интеллектуальной системы для задач ситуационного упреждающего управления информационной безопасностью // Естественные и технические науки. – 2016. – № 6. – С. 194-202.

7. Котенко И.В., Саенко И.Б., Чернов А.В., Бутакова М.А. Построение многоуровневой интеллектуальной системы обеспечения информационной безопасности для автоматизированных систем железнодорожного транспорта // Труды СПИИРАН. – 2013. – № 7. – С. 7-25.

8. Бирюков Д.Н., Ломако А.Г. Денотационная семантика контекстов знаний при онтологическом моделировании предметных областей конфликта // Труды СПИИРАН. – 2015. – № 5. – С. 155-179.

9. Аксененко Ю.И., Василенко В.В., Сидак А.А. Методологический подход к построению комплексных систем мониторинга и реагирования на инциденты информационной безопасности // Стратегическая стабильность. – 2018. – № 1. – С. 64-67.

10. Корниенко А.А., Бирюков Д.Н., Глухарев М.Л., Глухов А.П., Диасамидзе С.В. Модель онтологического представления процессов и метод синтеза спецификаций для интеллектуальной системы риск-ориентированного упреждающего управления информационной безопасностью // Известия ПГУПС, вып. 1, – 2018г., – С. 152-160.

11. Ададуров С.Е., Глухов А.П., Сидак А.А., Лыков В.В., Павлов А.Г. Рекомендации по проектированию компонентов микропроцессорных систем железнодорожной автоматики и телемеханики с учетом требований информационной безопасности // Двойные технологии. – 2018. – № 4. – С. 94-98.

12. Бирюков Д.Н., Ломако А.Г., Ростовцев Ю.Г. Облик антиципирующих систем предотвращения рисков реализации киберугроз // Труды СПИИРАН. – 2015. – № 2. – С. 5-25.

13. Бирюков Д.Н., Глухов А.П., Сабиров Т.Р., Пилькевич С.В. Модель изменения доступности знаний, представленных в памяти киберсистемы, обеспечивающей нейтрализацию деструктивных воздействий на объекты критической информационной инфраструктуры // Наукоемкие технологии в космических исследованиях Земли. – 2016.

– Часть 8. – № 4. – С. 56-63.
14. Бирюков Д.Н., Глухов А.П., Сабиров Т.Р., Пилькевич С.В. Подход к обработке знаний в памяти интеллектуальной системы // Естественные и технические науки. – 2015. – № 11. – С. 455-466.
15. Сидак А.А. Определение актуальных угроз безопасности информации в автоматизированных системах // Двойные технологии. 2018. № 1. С. 73-75.
16. Корниенко А.А., Глухов А.П., Диасамидзе С.В., Поляничко М.А., Бирюков Д.Н. Концептуальная модель интеллектуальной системы риск – ориентированного упреждающего управления информационной безопасностью железнодорожного транспорта // Естественные и технические науки.– 2017.– № 11.– С. 268-274.
17. Глухов А.П. Полумарковские модели оценивания вероятностно-временных характеристик выполнения функциональных задач автоматизированными системами управления критического применения // Естественные и технические науки. – 2015. – № 7. – С. 101-110.
18. Сидак А.А. Вопросы структуризации автоматизированных систем при организации защиты информации // Информационные войны. – 2018. – № 1. – С. 88-90.
19. Сидак А.А. Формирование функциональных требований безопасности, предъявляемых к защите информации в автоматизированных системах. Показатели затрат и риска // Стратегическая стабильность. – 2019. – № 1. – С. 41-42.
20. Сидак А.А. Сквозная реализация функциональных требований безопасности за счет обеспечения специальных свойств автоматизированных систем. Показатели эквифинальности // Стратегическая стабильность. – 2019. – № 2. – С. 62-65.

Материал поступил в редакцию 07 07. 2019 г.

УДК 681.3.06 (075.32)

© Усатенко Т.О.
© Usatenko T.

РАЗРАБОТКА МАТЕМАТИЧЕСКОЙ МОДЕЛИ КАСКАДНОГО ФИЛЬТРА КЛАССИФИКАЦИИ НЕЧЕТКИХ ОБЪЕКТОВ С ПРОМЕЖУТОЧНЫМИ СОСТОЯНИЯМИ

DEVELOPMENT OF THE MATHEMATICAL MODEL OF THE CASCADE FILTER CLASSIFICATION OF FUZZY OBJECTS WITH INTERMEDIATE CONDITIONS

Аннотация. *В рамках современного подхода к совершенствованию теории классификации и кластеризации нечетких признаков однозначно не идентифицируемых объектов предлагается математическая модель каскадного фильтра классификации нечетких объектов с промежуточными состояниями на основе теории категорий.*

Abstract. *In the framework of the modern approach to improving the theory of classification and clustering of fuzzy features of uniquely unidentifiable objects, a mathematical model of a cascade filter for the classification of fuzzy objects with intermediate states based on category theory is proposed.*

Ключевые слова. *Классификация, кластеризация, категория, функтор.*

Key words. *Classification, clustering, category, functor.*

В основу разрабатываемых теоретических основ входит ряд фундаментальных и специальных (прикладных) теорий, существо которых позволит ввести ряд определений, теорем и утверждений, необходимых для решения поставленной научной проблемы. При решении задачи классификации исследуемые технические системы с присущими им свойствами и характеристиками рассматриваются с точки зрения алгебраических объектов разного рода, например, таких как множества, группы и т.д. При этом для каждого такого рода объектов между ними определяются различного рода отображения (гомоморфизмы, изоморфизмы и др.) [1, 2]. Существенной особенностью является то, что данные отображения могут быть как четкого, так и нечеткого характера. Некоторые формальные свойства для отображений и объектов являются общими для них всех, например, существование тождественных отображений. Таким образом, разработку понятийного аппарата целесообразно проводить с точки зрения рассмотрения нечетких объектов и отображений как абстрактных категорий с последующим переходом к реальным объектам. Такой подход частично реализован при разработке теоретико-множественных оснований теории классификации [3]. Однако понятийно-категориальный аппарат, разработанный и использованный в данной теории, имеет ограниченное практическое применение и требует дальнейшего развития. С этой цель в настоящей работе предлагается увеличить масштаб абстрактных алгебраических конструкций, которые могут быть обоснованно модифицированы и задействованы в качестве теоретических основ решения классификационных задач с нечеткими признаками.

В качестве фундаментальной теоретической платформы решения поставленной научной проблемы предлагается использовать основные алгебраические конструкции теории категорий. Адекватность выбора данной теории обусловлена ее фрагментарным использованием в ряде работ, посвященных решению задачи классификации [2, 3]. Например, рассмотрение некоторых признаков и свойств систем, как и самих систем в целом, осуществляется с использованием математического аппарата теории множеств, являющегося одним из компонентов теории категорий. Таким образом, выбор и использование теории категорий в данном случае является логически обоснованным научным подходом, индуцированным предшествующими разработками в исследуемой предметной области.

Впервые понятие категории и функтора были определены известными европейскими математиками С. Маклейном и С. Эйленбергом в связи с имеющимися в то время актуальными математическими проблемами аксиоматизации теории групп гомологий и когомологий топологических пространств [5]. Данные понятия нашли широкое применение как в различных областях математики, так и в других научных направлениях [4, 1].

Введем ряд определений.

Определение 1. Однозначно не идентифицируемый объект A – объект любой природы, характеристическая функция которого относительно его принадлежности объекту A' имеет вид $f(A)\in[0;1]$.

В данном случае принадлежность представляет собой субъективную меру того, насколько однозначно не идентифицируемый объект A соответствует объекту A', смысл которого формализуется в зависимости от условий решаемой задачи.

Усатенко Тимур Олегович *– преподаватель, отдел РВСН УВЦ ,Московский авиационный институт, тел. +7(926)351-27-74.*

Usatenko Timur *– lecturer, department of the strategic missile forces of the UCC, Moscow Aviation Institute, tel. +7 (926) 351-27-74.*