МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

### Национальный исследовательский ядерный университет «МИФИ»

Институт

интеллектуальных кибернетических систем

### Кафедра кибернетики (№ 22)

### Направление подготовки 09.03.04 Программная инженерия

### РЕФЕРАТ ПО ДИСЦИПЛИНЕ «ВВЕДЕНИЕ В ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»

### Тема: «Применение интеллектуальных систем в сфере компьютерной безопасности»

Преподаватель: д.т.н., профессор Рыбина Галина Валентиновна

Студент: Косенко Никита Игоревич

Группа: Б20-524

### Москва 2022

1

**Содержание**

1. [Введение](#_bookmark0) 3
2. [Борьба с киберугрозами в энергетической сфере](#_bookmark1) 4
   1. [Экспертная система “Cyber”](#_bookmark2) 4
   2. [Интегрированные байесовские сети доверия](#_bookmark3) 5
   3. [Оценка рисков](#_bookmark4) 5
   4. [Работа всех трех ключевых компонент как единого целого](#_bookmark5) 6
3. [Интеллектуальные системы в кибербезопасности телекоммуникаций](#_bookmark7) 8
4. [Интеллектуальные системы и кибербезопасность в бизнес­среде](#_bookmark8) 9
5. [Другие идеи для применения интеллектуальных систем в кибербезопасности](#_bookmark9) 12
   1. [Концепция интеллектуальной системы обеспечения кибербезопасности сверх­](#_bookmark10) [звукового пассажирского самолета](#_bookmark10) 12
   2. [Разработка экспертной системы для контроля информационной безопасности](#_bookmark11) 13
   3. [Применение онтологий в информационных войнах](#_bookmark13) 15
   4. [Экспертные системы в кибербезопасности](#_bookmark15) 16
6. [Заключение](#_bookmark16) 17

# Введение

Обеспечение кибербезопасности на сегодняшний день является одной из наиболее акту­ альных проблем. Она давно поднялась с уровня частных лиц до уровня крупных организа­ ций. Возникла необходимость создания интеллектуальных систем (ИС), способных автома­ тизировать процесс анализа степени защищенности программного обеспечения этих орга­ низаций. Применение интеллектуальных систем в защите информационного пространства охватывает очень широкий круг направлений. В настоящий момент такие системы исполь­ зуются в следующих сферах [[1](#_bookmark17)]:

* + Обеспечение информационной безопасности энергетических обьектов
  + Обеспечение кибербезопасности бизнес­среды.
  + Системы обнаружения, предупреждения, реагирования на инциденты и ликвидацию последствий компьютерных атак.
  + Интеллектуальные системы антивирусной защиты, применяются для контроля кана­ лов проникновения вирусов, для защиты от вирусов, “червей”, нежелательных про­ грамм, для оповещения при “заражении”, для “лечения” от вирусов.

Вторые так же могут служить основанием для когнитивных подходов к оценке кибер­ безопасности [[2](#_bookmark18)].

Некоторые из проектов интеллектуальных систем по обеспечению компьютерной без­ опасности на данный момент существуют только в концептуальном виде [[13](#_bookmark29)], но есть и ре­ ализованные, основанные на онтологиях или технологии интеллектуальных многоагентных систем [[3](#_bookmark19)].

Цель данной работы — рассмотреть применение интеллектуальных систем для обес­ печения компьютерной безопасности различных общественных структур и изучить самые популярные подходы к построению такого рода систем.

# Борьба с киберугрозами в энергетической сфере

Одна из сфер, где наиболее востребованы интеллектуальные системы для поиска инфор­ мационных угроз является отрасль энергетики. Цифровизация ее объектов может вызвать возникновение киберугроз, связанных с внедрением новых решений, применением новых безнес­моделей, сопровождающихся отсутствием или недостаточностью информации для оперативного принятия решений по обеспечению безопасности объекта. Требования, предъ­ являемые к таким системам описаны в работе [[4](#_bookmark20)].

Построение ИС, ответственной за данную задачу, происходит по схеме, представленной в работах [[6](#_bookmark22), [7](#_bookmark23)]. Общая структура такой системы включает три компонента:

* + Экспертную систему (ЭС) “Cyber” – продукционная ЭС, предназначенную для выяв­ ления типовых уязвимостей, угроз и векторов атак ИТС объекта;
  + Блок байесовских сетей доверия, ответственный за моделирование экстремальных си­ туаций, вызванных нарушением кибербезопасности, определения вероятности наступ­ ления последствий;
  + Блок оценки рисков наступления экстремальной ситуации и последствий от реализа­ ции киберугроз

## Экспертная система “Cyber”

В работе [[5](#_bookmark21)] архитектура экспертной системы “Cyber” рассмотрена более подробно. Раз­ работка интеллектуальной системы основана на методике анализа угроз и оценки рисков нарушения информационной безопасности энергетических комплексов [[8](#_bookmark24)]. Экспертную си­ стему было решено проектировать с использованием продукционной модели знаний, кото­ рая позволяет отобразить экспертные данные в базе знаний в виде правил ЕСЛИ – ТО. ЭС включает три структурных элемента:

* + - Графический интерфейс пользователя;
    - Интерфейс взаимодействия;
    - Ядро экспертной системы.

База знаний представляет собой совокупность шаблонов (DEFTEMPLATES) и правил (RULES), а также вспомогательных функций (FUNCTION), обеспечивающих организацию фактов в базе знаний. В системе заложены три группы правил:

* + - Правила определения угроз по выбранному ответу пользователя с отметкой уязвимо­ сти;
    - Правила вывода мер защиты ресурса от выявленных угроз для каждой уязвимости в за­ висимости от класса защищенности автоматизированной системы управления (АСУ);
    - Общие правила вывода мер защиты ресурса от выявленных угроз для каждой уязвимо­ сти.

Внутренний алгоритм работы ЭС “Cyber” состоит в следующем: система содержит ряд вопросов по безопасности автоматизированной системы управления предприятием с вари­ антами ответов. Ввод условий осуществляется посредством опрашивания пользователей с предложением вариантов ответов. Получив ответы пользователя, система вносит факты о наличии уязвимостей и угроз, связанных с реализацией выявленных уязвимостей, в базу зна­ ний.

Угрозы с высокой степенью представляют наибольший риск нарушения безопасности для предприятия. Факты, соответствующие низкой и средней степени угроз, удаляются из базы знаний. Для высокой степени угроз системой формируется набор мер по обеспечению безопасности и выводится на экран.

До начала основного опроса пользователю предлагается выбрать уровень защищенно­ сти АСУ, который влияет на критичность уязвимостей угроз и выбор меры обеспечения без­ опасности.

## Интегрированные байесовские сети доверия

Байесовские сети доверия (БСД) отвечают за построение сценариев вероятных угроз. Для БСД разработана онтология сценария экстремальной ситуации в энергетике, вызванной нарушением кибербезопасности на объекте. Такой сценарий представляет собой вероятност­ ные оценки возможных ситуаций, представленные последовательностью уязвимостей, кибе­ ругроз, угрозами причинения ущерба предприятию либо энергосистеме в целом. В процессе формирования графа экстремальной ситуации оценивается вероятность наступления некото­ рых негативных событий. В работе по исследованию энергетической безопасности [[9](#_bookmark25)] раз­ работаны опознавательные признаки, по которым система судит о наступлении ой или иной ситуации.

## Оценка рисков

Анализ рисков проводится в рамках решения задач по анализу киберугроз и моделирова­ нию сценариев экстремальных ситуаций в энергетике. После онтологического инжениринга система оценки рисков будет состоять из следующих компонент:

* + - Идентификация рисков (осуществляется при анализе угроз, поддерживаемой онтоло­ гией оценки рисков)
    - Анализ риска (осуществляется при моделировании сценариев, поддерживаемого онто­ логией оценки рисков)
    - Оценивание рисков (поддерживается онтологией критериев ранжирования, онтологи­ ей рисков кибербезопасности, онтологией рисков и критериев оценки)

В данном контексте риск рассматривается как сочетание последствий некоторого инцидента и связанной с ним возможностью возникновения. Оценка рисков — процесс идентификации, анализа и оценивания, в соответствии со стандартом ISO/IEC 27005:2011.

На заключительном этапе оценки рисков предполагается проводить ранжирование объ­ ектов. Для этого вводится критерий значимости объекта, зависящий от критерия оценки рис­ ков, интегрального показателя рисков объекта, объекта, представленного совокупностью ос­ новных характеристик.

## Работа всех трех ключевых компонент как единого целого

Основные задачи, которые решает интеллектуальная система: анализ киберугроз, моде­ лирование сценариев, и оценивание рисков. Для ее реализации была придумана совокуп­ ность систем онтологий, отвечающих за отдельные аспекты проблемы. Схема этой системы представлена на рис. [2.1](#_bookmark6).

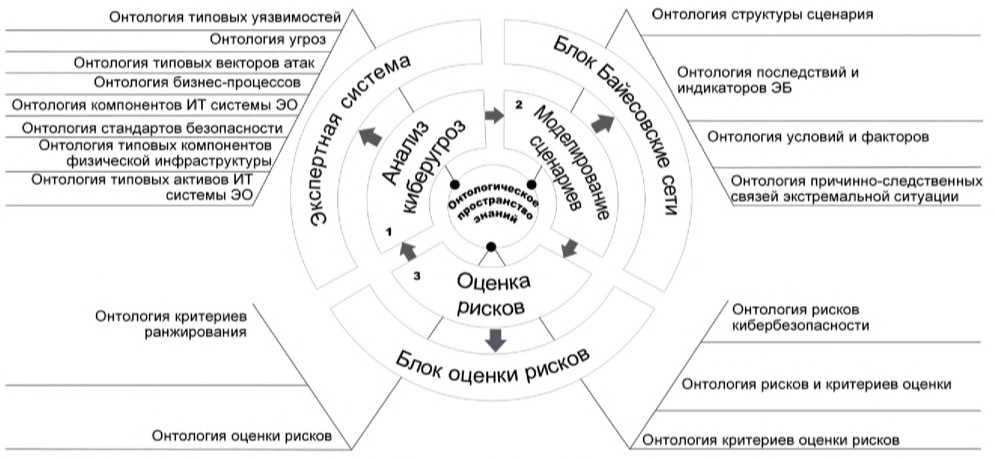


Рис. 2.1: Строение системы онтологий

Из данной схемы ясно, что для каждой из основных предметных областей создается на­ бор онтологий, связанных между собой. В разделе, связанным с анализом киберугроз, онто­ логический инжениринг позволяет систематизировать информацию об различных информа­ ционно­технологических характеристиках конкретных энергетических объектов и создать базу знаний их уязвимостей и угроз.

**Онтология стандартов безопасности** разрабатывается с целью кластеризации знаний по методам проведения оценки безопасности. Впоследствии она послужит компонентом для проведения аудита безопасности предприятий, проводимого с использованием “Cyber” и мо­ делировании сценариев возможных экстремальных ситуаций.

За определение основных угроз в системе антологий, предлагаемой в работе [[7](#_bookmark23)], отвеча­ ет **онтология угроз**. Ключевая задача этой онтологии — установление самых актуальных уязвимостей в энергетике.

После полного цикла работы данной интеллектуальной системы пользователь получа­ ет список объектов энергетики, упорядоченный по степени уязвимости к кибератакам или иным экстремальным ситуациям в области кибербезопасности.

# Интеллектуальные системы в кибербезопасности телеком­ муникаций

Большинство современных систем кибербезопасности (КБ) телекоммуникационных се­ тей и технологий (ТКСиТ) являются сложными управляемыми системами [[10](#_bookmark26)], разработка которых требует постоянного анализа тенденций их развития, направлений совершенствова­ ния технологий их построения. В отличие от процесса разработки системы кибербезопасно­ сти ТКСиТ, реализация которого требует принятия технических решений по всему перечню решаемых задач проектирования различными специалистами (группами специалистов), про­ цесс экспертной деятельности должен быть направлен на формирование экспертных оценок, основанных на анализе некоторых обобщенных показателей качества проектируемой систе­ мы, характеризующих стратегические технические решения (технические решения, опреде­ ляющие облик системы кибербезопасности в целом) и осуществляется сравнительно неболь­ шой группой специалистов.

Суть подхода заключается в формировании экспертных показателей качества (ЭПК), от­ ражающих уровень КБ и существенные свойства СКБ ТКСиТ, формировании оптимальных (не избыточных) экспертных систем показателей качества (ЭСПК), соответствующих физи­ ческому, канальному и сетевому уровню кибербезопасности ТКСиТ, на основе моделей и алгоритмов, соответствующих характеру и степени априорной неопределенности того или иного этапа функционирования данной системы. Очевидно, что реализовать предложенные модели и методы в ходе организации экспертной деятельности в интересах анализа кибербез­ опасности ТКСиТ возможно только на основе разработки специальных экспертных систем. Основу знаний, содержащихся в специальной ЭС должны, на наш взгляд, составлять знания: содержащиеся в памяти эксперта­донора; полученные в результате моделирования процессов изменения ЭПК КБ ТКСиТ; полученные в результате анализа данных, поступаю­ щих из системы­аналога; содержащиеся на материальных носителях (компакт диски, специ­ альная литература и т.д.). В настоящее время разработаны десятки моделей (языков) пред­ ставления знаний для различных предметных областей. Все многообразие моделей можно разбить на две большие группы – модульные и сетевые. Поскольку модульные модели опе­ рируют совокупностью не связанных элементов знаний и предназначены для интерпретации только поверхностных знаний в специальной ЭС такого класса должны быть реализованы

сетевые языки представления знаний.

# Интеллектуальные системы и кибербезопасность в биз­ нес­среде

Второй, но оттого не менее важной областью применения ИС для обеспечения инфор­ мационной безопасности является бизнес­среда. В данном случае многоагентный подход находит широкое применение в областях, требующих решения сложных задач: реинжини­ ринг бизнес­процессов, построение виртуальных предприятий, имитационное моделирова­ ние интегрированных производственных систем и т.д [[11](#_bookmark27)]. Наибольшую сложность в теоре­ тических исследованиях и практических реализациях современных многоагентных систем представляют вопросы, связанные с обеспечением информационной безопасности агентов и информационных ресурсов, которыми они оперируют, в открытых многоагентных вирту­ альных средах.

В качестве примера автор работы [[11](#_bookmark27)] приводит решение задачи обеспечения инфор­ мационной безопасности в объектах многоагентной системы информационной поддержки инноваций, реализующей открытую многоагентную виртуальную бизнес­среду инноваци­ онной деятельности.

С точки зрения общей логики функционирования такая среда имеет многоагентную реа­ лизацию. Агентная ориентированность выражается в том, что в ней каждый субъект иннова­ ционной деятельности представлен одним или несколькими мобильными агентами, которые представляют предложения своих владельцев и реализуют процедуры автоматизированного поиска партнеров для сотрудничества.

В общем случае такая многоагентная система, какая описана в работе [[11](#_bookmark27)], задается отно­ шением множеств пользователей системы, ее агентов, представляющих их интересы в биз­ нес­среде, множества узлов системы, множества виртуальных бизнес­площадок, множества информационных ресурсов системы, множества атрибутов объектов модели. Два основных типа агентов системы: мобильные агенты и управляющие агенты. Первые перемещаются между узлами сети, а вторые координируют процессы взаимодействия и миграции первых.

Для решения задачи обеспечения кибербезопасности в распределенной многоагентной системе авторами статьи [[11](#_bookmark27)] предлагается метод формирования комплексной самоорганизу­ ющейся системы децентрализованного управления безопасностью мобильных агентов, аутен­ тификация мобильных агентов в которой осуществляется через открытые ключи и удостове­ ряющие их центры.

В предлагаемой системе формирование удостоверяющих центров будет осуществлять­ ся автоматически на основе механизмов самоорганизации агентов а функции управления процедурой выдачи сертификатов будут возложены на программных управляющих агентов. Самоорганизация заключается в автоматическом формировании виртуальных площадок, объединяющих агентов с близкими целями в коалиции, и генерации управляющих агентов,

выполняющих функции удостоверяющих центров сертификации, для каждой площадки.

Система безопасности мобильных агентов может быть как централизованной, так и де­ централизованной.

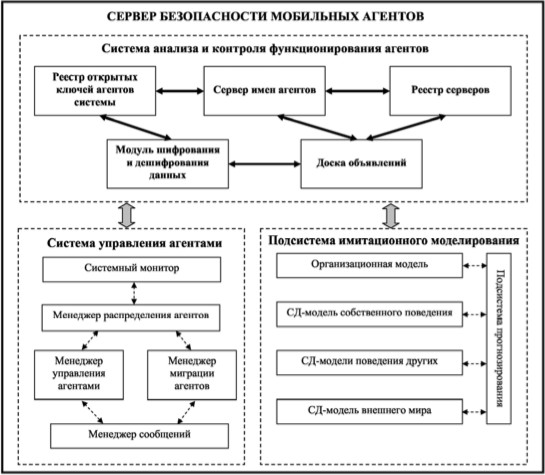


Рис. 4.1: Система безопасности мобильного агента(под централизованным управлением) [[11](#_bookmark27)]

В случае использования системы с **централизованным** управлением безопасностью мобильных агентов в открытой многоагентной виртуальной бизнес­среде, оно реализуется на выделенном сервере, функциональная структура которого состоит в следующем: сервер безопасности мобильных агентов обеспечивает централизованное хранение информации об агентах системы, доступных узлах, виртуальных бизнес­площадках, открытых ключах аген­ тов, доступ к которым имеют только управляющие агенты системы. Здесь же реализуются модуль шифрования и дешифрования данных, а также система мониторинга, анализа и мо­ делирования поведения агентов системы, которая также доступна управляющим агентам си­ стемы.

В случае использования системы с **децентрализованным** подходом управление без­ опасностью мобильных агентов в виртуальной бизнес­среде реализуется на каждом из сер­ верных узлов системы (порталов), на которых пользователи регистрируют свои предложе­ ния. При таком решении система безопасности мобильных агентов является частью агент­ ного представительства серверного узла и выполняет аналогичные функции, что и сервер безопасности мобильных агентов: хранит информацию об агентах системы, доступных уз­ лах, виртуальных бизнес­площадках, открытых ключах агентов, доступ к которым имеют только управляющие агенты системы, реализует процедуры шифрования и дешифрования данных агентов, осуществляет мониторинг, анализ и моделирование поведения агентов си­ стемы.

Централизованная система в сравнении с децентрализованной обладает рядом недостат­ ков [[12](#_bookmark28)]:

1. уязвимость центрального звена (при отказе сервера безопасности нарушается защита активных компонентов и всей системы в целом, ее безопасность становится под угро­ зой);
2. высокая нагрузка на центральный сервер управления безопасностью при большом ко­ личестве агентов и узлов и, как следствие – ограниченная масштабируемость;
3. централизованное администрирование подразумевает полный контроль над ресурса­ ми на стороне сервера, что не всегда приемлемо, если ресурсы принадлежат разным пользователям

Помимо описанных выше минусов, согласно работе [[11](#_bookmark27)], централизованное управление безопасностью гораздо менее продуктивно и намного более длительно чем децентрализо­ ванное. При увеличении количества узлов и мобильных агентов увеличивается нагрузка на центральный сервер безопасности мобильных агентов, тем самым уменьшается производи­ тельность МАС.

Ввиду описанных выше аспектов, использование децентрализованной системы для обес­ печения безопасности мобильных агентов предпочтительно.

# Другие идеи для применения интеллектуальных систем в кибербезопасности

Интеллектуальные системы применяются в контексте кибербезопасности не только в тех областях, о которых было написано выше. Существуют и не совсем обычные проекты, связанные с этой отраслью.

## Концепция интеллектуальной системы обеспечения кибербезопас­ ности сверхзвукового пассажирского самолета

Конструктивное решение по обеспечению информационной безопасности воздушного средства (ВС), должно гарантировать невозможность перехвата управления и нарушение ра­ ботоспособности оборудования и систем ВС ( Это решение так же должно реализовывать такие требования безопасности как контроль и управление доступом, обеспечение целостно­ сти ресурсов, обеспечение защиты конфиденциальности при хранении и передачи информа­ ции и др. ) [[13](#_bookmark29)]. Так же система обеспечения кибербезопасности должна иметь возможность функционировать в условиях реального времени и использовании современных технологий сотовой, спутниковой и радиосвязи для передачи больших объемов данных. Для предотвра­ щения потенциальных киберинцидентов необходимо использовать комплексный подход к управлению киберрисками ВС. Данный подход должен включать в себя последовательный ряд процедурных и технических решений по предотвращению киберинцидентов и послед­ ствий от них. Он будет состоять из следующих этапов:

* + 1. Выявление угроз (внутренних и внешних)
    2. Идентификация уязвимостей (Определение перечня бортового оборудования, имею­ щего проводные / беспроводные каналы информационного взаимодействия. Прогноз возможных последствий угроз кибербезопасности каждой системы. Определение воз­ можностей и ограничений применения на борту ВС существующих способов защиты.)
    3. Оценка подверженности рискам (Определение вероятности уязвимости от внешних / внутренних угроз, ошибки при создании и закладки ПО, преднамеренное / непредна­ меренное негативное влияние человека при эксплуатации оборудования)
    4. Разработка способов обнаружения и защиты (Снижение вероятности уязвимости через защитные меры. Уменьшение потенциального воздействия уязвимостей при эксплуа­ тации)
    5. Локализация отказа и сохранение безопасной эксплуатации (Разработка алгоритма ло­ кализации последствий киберинцидента, реконфигурация оборудования для сохране­ ния безопасной эксплуатации ВС, сниение любого потенциала выявленных киберрис­ ков.)
    6. Очистка и восстановление после киберинцидента (Разработка алгоритма действий по устранению последствий киберинцидента и восстановлению системы.)

Одной из перспективных систем организации воздушного движения, направленных на интеграцию будущих систем связи, навигации, наблюдения и управления воздушным дви­ жением (УВД), осуществляемую на базе общесистемного управления информации, является система SWIM (System Wide Information Management) [[13](#_bookmark29)]. SWIM предназначена для обмена данными и направлена на предоставление дополнительных услуг по управлению информа­ цией организации воздушного движения с использованием внешних сервисов ВС. Архитек­ тура SWIM построена на базе сервис­ориентированной архитектуры SOA (Service Oriented Architecture) [[14](#_bookmark30)].

Программные комплексы, разработанные в соответствии с SOA, обычно реализуется как набор веб­служб, взаимодействующих по протоколам SOAP, REST, XML. Основные пре­ имущества использования веб­сервисов на основе SOA: возможности расширения системы за счет модульности и автономности бизнес­серверов; адаптивная настройка логики рабо­ ты системы и изменение состава используемых компонентов без перекрытия; повышение безопасности авиаперелетов за счет стандартизации процедур и протоколов для управления сетевой и сервисной интеграции; безопасная интеграция с платформами и приложениями; уменьшение стоимости и времени реализации проектов.

Архитектура SOA может быть реализована с использованием как сервисной, так и мик­ росервисной архитектуры приложений. Поддержка микросервисов позволяет использовать концепцию “блокчейн как микросервис и передачу данных осуществлять в единой блокчейн инфраструктуре с открытым исходным кодом, которая устраняет недостатки АЗН­В [[15](#_bookmark31)] и обеспечивает высокий уровень доверия между участниками сервисного обмена.

Согласно [[13](#_bookmark29)], внедрение блокчейн технологий увеличивает скорость обмена, уменьша­ ет временные затраты, улучшает качество, надежность и доступность услуг. При этом уве­ личивается прозрачность и надежность передачи информации, снижаются киберриски.

Реализация предлагаемой концепции интеллектуальной системы обеспечения кибербез­ опасности бортового оборудования и систем СПС, построенной на базе архитектуры SOA с использованием блокчейн технологий, позволит сохранить работоспособность авиацион­ ных систем и оборудования, повысить безопасность полетов, предотвратить человеческие жертвы и повысить степень комфорта пассажиров при возникновении киберугроз на борту во время полета.

## Разработка экспертной системы для контроля информационной без­ опасности

Работы [[6](#_bookmark22), [7](#_bookmark23)] интегрировали в свои интеллектуальные системы экспертную систему “Cy­ ber”. Но они не единственные, кто принял решение внедрить экспертную систему в область безопасности информационного пространства. В работе [[16](#_bookmark32)] автор, ориентируясь на различ­ ные банковские и бизнесс структуры, делает акцент на доступности экспертной системы для

пользователя. Поэтому он предлагает собственную архитектуру экспертной системы (рис. [5.1](#_bookmark12)). Такая архитектура позволяет упростить работу с экспертной системой как со стороны пользователей, так и со стороны ее проектировщиков.

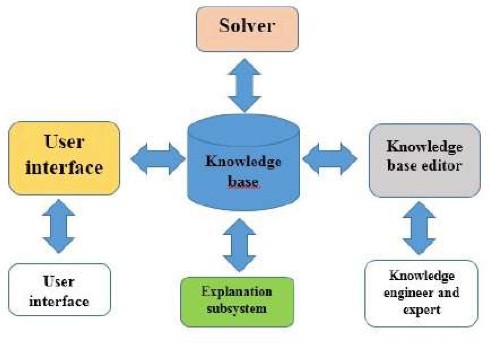


Рис. 5.1: Архитектура экспертной системы [[16](#_bookmark32)]

Разработка данной экспертной системы состоит из нескольких этапов:

* + 1. Идентификация
    2. Концептуализация
    3. Формализация
    4. Реализация
    5. Тестирование
    6. Опытная эксплуатация

На этапе **идентификации** определяются решаемые задачи, определяются цели разработ­ ки, определяются эксперты и типы пользователей. Во время **концептуализации** проводится содержательный анализ проблемной области, выявляются используемые понятия и их взаи­ мосвязи, определяются методы решения проблемы. После этого при **формализации** выбира­ ются и определяются способы представления всех видов знаний, формализуются основные понятия, определяются способы интерпретации знаний, моделируется работа системы, спо­ собы представления и манипуляции знаниями.

После этого наступает длительная ступень **реализации**. На этом этапе база знаний за­ полняется экспертами и эта часть процесса самая важная и трудоемкая, поскольку происхо­ дит упорядочение знаний, полученных от экспертов, что обеспечивает эффективную работу системы в дальнейшем и представление знаний в виде ЭС. Реализация выполняется инжене­ ром по знаниям. Стоит помнить, что начиная с этого этапа могут возникнуть определенного рода проблемы [[16](#_bookmark32)].

Следующим шагом на пути к претворению в жизнь экспертной системы станут различ­ ного рода **тесты**. На этом этапе выделяются ключевые проблемы проектируемой системы:

какую информацию защищать, где она расположена в базе знаний, какие устройства пользу­ ются базой знаний, достаточно ли надежны пароли, задаваемые пользователями и т. д... Для их решения задаются необходимые переменные и строятся логические блоки с ветвлениями. После этого получается готовый продукт, достаточно удобный для потребителей.

## Применение онтологий в информационных войнах

Понятие информационной войны подразумевает использование информационных и ком­ муникационных технологий для достижения преимуществ по сравнению с потенциальным противником. В данном контексте информационные структуры рассматриваются как систе­ мы, хранящие информацию, обрабатывающие ее и определяющие, представляет тот или иной пакет угрозу или нет. Для этой цели используется онтологический подход к созданию интеллектуальной системы, предоставляющей базу знаний для потенциального обучения на ней нейронной сети [[17](#_bookmark33)] или иной самообучающейся системы.

Структура антологии, описанной в работе [[18](#_bookmark34)] базируется модели идентификации угроз STRIDE и методики DREAD для оценки рисков угроз. В работе [[17](#_bookmark33)] она присутстсвует в упрощенном виде (см рис. [5.2](#_bookmark14)).

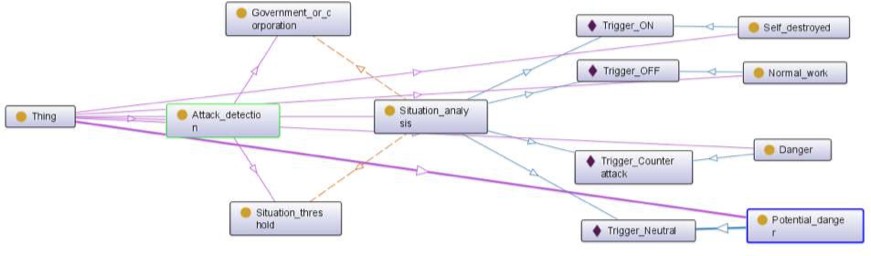


Рис. 5.2: Структура онтологии для определения угроз [[17](#_bookmark33)]

В данной схеме Attack­detection есть абстрактный класс, включающий в себя ключевые аспекты предметной области: Government or corporation (подкласс, определяющий к како­ му типу угроз относится поступающая угроза), Situation analysis (подкласс, анализирующий ситуацию), различные тригеры, отражающие выводы к которым пришла самообучающаяся система в результате анализа ситуации (“ON” — триггер немедленной остановки анализа и признания атаки угрозой, “OFF” — система воспринимает атаку как ложную и продолжа­ ет функционировать, “NEUTRAL” — атака воспринимается как неизвестная потенциальная опасность, система продолжает функционировать, но в отличие от “OFF” происходит более глубокий анализ атаки и причин ее возникновения с целью их последующего устранения, ““COUNTERATTACK” — атака расценивается как угроза, дальнейшие действия становятся непредсказуемы)

Таким образом онтология, описанная выше, ложится в основу самообучающейся систе­ мы, способной идентифицировать различные киберугрозы.

## Экспертные системы в кибербезопасности

Существуют и проекты, посвященные оптимизации и ускорению процесса принятия ре­ шений. Учитывая постоянное возрастание многообразия потенциальных и сложности реаль­ ных киберугроз, одним из вариантов повышения эффективности принятия решений в обла­ сти защиты информации (ЗИ) и кибербезопасности стало внедрение разнообразных интел­ лектуальных (или интеллектуализированных) программно­аппаратных комплексов в данной области.

По мере усложнения сценариев кибератак стало очевидно [[19](#_bookmark35)], что традиционные сиг­ натурные методы не всегда в состоянии обеспечить должный уровень защиты объектов ин­ форматизации.

Ключевая особенность подхода, который используется в проектируемой АЭС(адаптивной экспертной системы), –– применение ДПРПУ. Это позволило получать довольно высокие результаты в ходе тестовых экспериментов по распознаванию разновариантных угроз, ано­ малий и кибератак.

Сравнивая с широко используемыми в системах выявления вторжений (кибератак) мето­ дами и моделями (последовательный перебор признаков, статистические алгоритмы состоя­ ний), модели, которые в своей основе содержали ДПРПУ, а также разнообразные ОИО, дали значительный эффект. Так, в частности, сократился объем необходимых правил для распо­ знавания ОБР. Например, в рамках класса сокращение правил составило 2,5–12 раз (зависит от класса ОБР – аномалия, кибератака, киберугроза)

Следовательно, возможно добиться существенного снижения времени выяв­ ления ано­ малий, кибератак или угроз, а также последующей оценки их последствий для ОБИ.

# Заключение

В заключении стоит сказать, что применение интеллектуальных систем в области ком­ пьютерной безопасности достаточно широко. Были рассмотрены как уже созданные модели ИС, так и концепции, которые могут быть реализованы в будущем. По итогам работы можно сделать вывод, что чаще всего ИС, ответственные за кибербезопасность основаны на онтоло­ гиях, на многоагентных системах либо на экспертных системах. Возможность использовать несколько компонентов сразу тоже вполне реальна.

Существуют и проекты, использующие либо оригинальные базы знаний и архитекту­ ры, либо основанные на готовых продуктах [[13](#_bookmark29), [17](#_bookmark33)]. Применяются они в банковской сфере, в бизнесе, на энергетических объектах, а так же потенциально могут быть применены и в транспортной сети.

Но работа таких интеллектуальных систем далеко не всегда бывает быстрой и продук­ тивной [[11](#_bookmark27), [20](#_bookmark36)]. Это означает, что следует и дальше развивать рассмотренные в данной рабо­ те технологии использования интеллектуальных систем для обеспечения безопасности ин­ формационного пространства как крупных организаций и компаний, так и частных лиц.

# Список литературы

1. V. Tabakaeva, V. Selifanov, V. An, S. Bularga, and A. Vorozhtsov, Intelligent information se­ curity management systems, Trans. Sci. Pap. Novosib. State Tech. Univ., vol. 4, no. 3–4, pp. 165–176., ­2020
2. Бурый А.С., Усцелемов В.Н. Онтологический подход к формированию когнитивных мо­ делей оценки кибербезопасности // Информационно­экономические аспекты стандарти­ зации и технического регулирования., No 3. (55). С. 77­84., ­2020.
3. И. В. Котенко, Интеллектуальные механизмы управления кибербезопасностью, ­2009.
4. Ворожцова Т. Н., Онтология как основа для разработки интеллектуальной системы обес­ печения кибербезопасности // Онтология проектирования., C.69­77., ­2014
5. А. Г. Массель, Д. А. Гаськова,Разработка экспертной системы для анализа угроз кибер­ безопасности в энергетических системах // Information and mathematical technologies in science and management, No 1 (27), pp. 113­122, ­2016
6. D. Gaskova, A. Massel, The Technology of Cyber Threat Analysis and Risk Assessment of Cybersecurity Violation of Critical Infrastructure // Vopr. kiberbezopasnosti, vol. 2, no. 2(30), pp. 42–49, ­2019
7. А. Г. Массель, Д. А. Гаськова, Онтологический инжениринг для разработки интеллекту­ альной системы анализа угроз и оценки рисков кибербезопасности энергетических объек­ тов // Онтология проектирования, C. 255­238., ­2019
8. А. Г. Массель, Методика анализа угроз и оценки риска нарушения информационно­ технологической безопасности энергетических комплексов // XX Байкальской Всероссий­ ской конференции:труды, т. III., С. 186­195., ­2015.
9. Н И Пяткова, В И Рабчук, С М Сендеров, Энергетикая безопасность России: проблемы и пути решения / Новосибирск: СО РАН, С. 198, ­2011
10. Малофеев В. А., Паращук И. Б., Пронин А. А., Саяркин Л. А., Экспертные системы для анализа кибербезопасности телекоммуникационных сетей и технологий, их задачи и особенности // ХVII САНКТ­ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ,

С. 114­115., ­2020

1. А.В. Маслобоев, В.А. Путилов, Разработка и реализация механизмов управления ин­ формационной безопасностью мобильных агентов в распределенных мультиагентных ин­ формационных системах // Вестник МГТУ, том 13, №4/2, C. 1015­1032, ­2010
2. А.В. Маслобоев, М.Г. Шишаев , Одноранговая распределенная мультиагентная систе­ ма информационноаналитической поддержки инновационной деятельности // Научно­ технический вестник СПбГУ ИТМО, № 4(62), C.108­114, ­2009.
3. Зыбин Е.Ю., Кривоноженков В.А., Муллин А.Р., Кохан В.В., Концепция интеллектуаль­ ной системы обеспечения кибербезопасности бортового оборудования и систем сверхзву­ кового пассажирского самолета, ФГУП “ГосНИИАС”, ­2021
4. Z. Wang, X. Luo, M. Zhao and M. Qi, The research of system wide information manage­ ment based on SOA // 6th IEEE International Conference on Software Engineering and Service Science (ICSESS), pp. 837­840., ­2015
5. Косьянчук В.В., Сельвесюк Н.И., Хамматов Р.Р. Обзор основных путей повышения без­ опасности системы АЗН­В // Научный Вестник МГТУ ГА. 2019. Том 22, №01. С. 39­48.
6. T. Marzhan, Method of development of information security expert system, ­2019, [Online].

Available: https://proc.ostis.net/wp­content/uploads/2019/10/OSTIS­2019.pdf

1. Научные Труды Конференции, “Open Semantic Technologies for Intelligent Systems” // Inf.Tsu.Ru, vol. 7740, no. 3, pp. 145­150, ­2019, [Online]. Available: [http://www.inf.tsu.ru/library/Publications/2020/2020­139.PDF](http://www.inf.tsu.ru/library/Publications/2020/2020).
2. P. Grabusts, O. Uzhga­Rebrov, Ontology­Based Risk Analysis System Concept. // Open se­ mantic technologies for intelligent systems, OSTIS­2017, Minsk, Belarus, pp. 341­346, ­2017.
3. Ахметов Б.С., Лахно В.А., Досжанова А.А., Картбаев Т.С., Сабит Б. Модели для адап­ тивной экспертной системы по выявлению киберугроз. // Проблемы информатики в об­ разовании, управлении, экономике и технике: Сб. статей XVIII Междунар. научно­техн. конф. Пенза: ПДЗ, С. 84­90., 2018.
4. Коломойцев В.С., Богатырев В.А., Поляков В.И., Open Semantic Technologies for In­ telligent Systems // Inf.Tsu.Ru, vol. 7740, no. 3, pp. 315­320, ­2019, [Online]. Available: [http://www.inf.tsu.ru/library/Publications/2020/2020­139.PDF](http://www.inf.tsu.ru/library/Publications/2020/2020).