Лекция №3

Тема: Интеллектуализация систем защиты информации

План:

1. **Основные понятие интеллектуализация систем защиты информации**
2. **Функциональная организации интеллектуальной системы управление**
3. **Архитектура перспективной интеллектуальной системы защиты информации**

Ключевые слова:

Диалоговое общение, Формирование цели, **подсистему обнаружения СПТВ, подсистему накопления данных, подсистему анализа защищенности, подсистему адаптации СЗИ, подсистему активного противодействия СПТВ.**

Интеллектуализация систем защиты информации

Под *интеллектуализацией* СЗИ будем понимать повышение ее интеллектуальных возможностей с целью обеспечения высокого уровня ее автономности, адаптивности и надежности в условиях неопределенности. Это предполагает передачу компьютеру максимально возможного количества функций по сбору, обработке информации и принятию решений для того, чтобы помочь пользователям и администраторам системы получить более объективную оценку событий, происходящих на объекте (в системе), и принять правильные и своевременные решения. В качестве средства борьбы с неопределенностью (НЕ-факторами) в данном случае выступают методы и технологии *искусственного интеллекта.*

Заметим, что в отношении точного определения ИИ, его возможностей и перспектив в последние годы не прекращаются споры. Так, известный специалист в области ИИ Джордж Ф. Люггер в своей книге пишет: «Проблема определения искусственного интеллекта сводится к проблеме определения интеллекта вообще: является ли он чем-то единым, или этот термин объединяет набор разрозненных способностей? В какой мере интеллект можно создать, а в какой он существует априори? Что именно происходит при таком создании?... Можно ли судить о наличии интеллекта только по наблюдаемому поведению, или же требуется свидетельство наличия некого скрытого механизма? Как представляются знания в нервных тканях живых существ, и как можно применить это в проектировании интеллектуальных устройств? ... И более того, необходимо ли создавать интеллектуальную компьютерную программу по образу и подобию человеческого разума, или же достаточно строго «инженерного» подхода?... На эти вопросы ответа пока не найдено, но все они помогли сформировать задачи и методологии, составляющие основу современного ИИ. Отчасти привлекательность искусственного интеллекта состоит в том, что он является оригинальным и мощным орудием для исследования именно этих проблем. ИИ представляет средство и испытательную модель для теорий интеллекта: такие теории могут быть переформулированы на языке компьютерных программ, а затем испытаны при их выполнении».

Термин «интеллектуальная система» также пока не получил общепринятого определения. Как правило, считается, что интеллектуальная система характеризуется наличием одного или нескольких из перечисленных ниже свойств:

- адаптивность;
- способность к обучению и самообучению;
- совершение «правильных действий»;
- ориентированность на определенную цель;

-использование знаний в процессе обучения и функционирования.

Для наглядности представим интеллектуальную систему в виде некоторой «интеллектуальной машины» (рис. 1.3), формирующей результат решения задачи *{действие)* на основе анализа и обработки поступающей входной информации *(восприятие)* с помощью определенной системы правил *(знаний)*

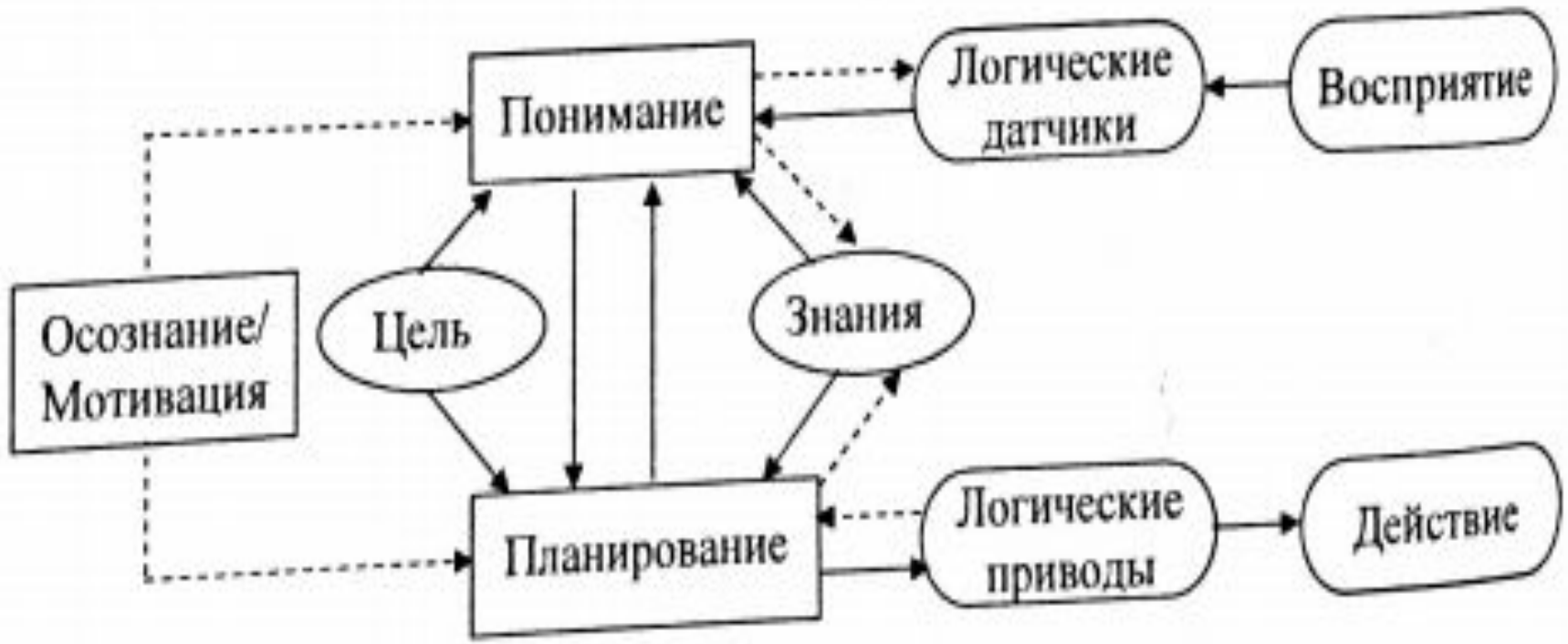

Рис. 1.3. Структура интеллектуальной машины

Логические датчики (сенсоры) и *логические приводы* (исполнительные механизмы) играют роль интерфейса с **внешней** средой (взаимодействующим объектом). В блоке ***понимания*** осуществляется сравнение текущего состояния объекта с *целью* (т.е. его желаемым состоянием), после чего производится *планирование,* т.е. принятие решения о выполнении некоторых действий, для уменьшения этого рассогласования при заданных ограничениях. Блок *осознания/мотивации* выполняет функцию слежения за пониманием и планированием. В случае если машина не может понять полученные с помощью логических датчиков данные, осознание / мотивация может приспособить (изменить) знания и сделать полученные данные более доступными для понимания. Таким образом, можно выделить два основных режима работы интеллектуальной системы (машины) - режим решения поставленной задачи и режим обучения / самообучения.

Под обучением понимается способность системы улучшать свое поведение в будущем, основываясь на экспериментальной информации, полученной в прошлом о результатах взаимодействия с объектом / окружающей средой. Самообучение — это обучение без внешней корректировки, т.е. без указаний «учителя».

Подводя краткий итог сказанному, процитируем получившее широкое распространение на практике определение : интеллектуальная система - это такая система, которая «способна понимать, делать выводы и обучаться в отношении процессов, возмущений и условий своего функционирования. Эта система накапливает свои знания и опыт, используя их для улучшения своих качественных характеристик».

Необходимым признаком интеллектуальной системы является наличие *базы знаний,* содержащей сведения (факты), модели и правила, позволяющие уточнить поставленную перед системой задачу и выбрать рациональный способ ее решения. Именно поэтому об интеллектуальных системах говорят как о системах, основанных на знаниях (англ. *Knowledge-Based Systems).* Для обеспечения свойства интеллектуальности системы необходимо придерживаться следующих принципов ее структурной организации :

1) наличие тесного информационного взаимодействия с реальным внешним миром и использование специально организованных информационных каналов связи;

2) принципиальная открытость системы для повышения интеллектуальности и совершенствования собственного поведения,

3) наличие механизмов прогноза изменений внешнего мира и собственного поведения системы в динамически меняющем внешнем мире и собственного поведения системы в динамический меняющемся внешнем мире;

4) наличие многоуровневой иерархической структуры построенной в соответствии с правилом: повышение интеллектуальности и снижение требований к точности моделей по повышения ранга иерархии(и наоборот);

5) сохраняемость функционирования (возможно, с некоторой потерей качества или эффективности) при разрыве связей или потере управляющих воздействий от внешних уровней иерархии в системе

Системы, организованные и функционирующие в соответствии со всеми пятью перечисленными принципами, называются системами, интеллектуальными «в большом».

Как видно из этого определения, система, интеллектуальная «в большом», должна иметь многоуровневую иерархическую структуру. Наиболее полно указанным выше требованиям удовлетворяет трехуровневая система управления, включающая в себя:

— исполнительный уровень;

— уровень координации (тактический уровень);

— уровень планирования (стратегический уровень).

Основные функции, реализуемые на данных уровнях

Системы, организованные и функционирующие в соответствии со всеми пятью перечисленными принципами, называются системами, интеллектуальными «в большом».

Как видно из этого определения, система, интеллектуальная «в большом», должна иметь многоуровневую иерархическую структуру. Наиболее полно указанным выше требованиям удовлетворяет трехуровневая система управления, включающая в себя:

— исполнительный уровень;

— уровень координации (тактический уровень);

— уровень планирования (стратегический уровень).

Основные функции, реализуемые на данных уровнях управления интеллектуальной системы, показаны на рис

Рис. 1.4. Схема функциональной организации интеллектуальной системы управления

Заметим, что в соответствии с четвертым выше принципов, называемым также принципом Саридиса и принципом *IPDI (Increasing Precision - Decreasing Intelligence),* п" мере продвижения к верхним уровням иерархии системы должен повышаться удельный вес ее интеллектуальных функций при одновременном снижении требований к точности их реализации. И наоборот, чем ниже по иерархии уровень управления, т.е. чем конкретнее решаемая задача, тем меньше знаний (и тем больше конкретных данных) требуется для ее решения.

Разумеется, степень интеллектуальности каждого из уровней управления может существенно различаться в зависимости от назначения системы и специфики решаемых с ее помощью задач. На практике возможно построение таких интеллектуальных систем, которые не удовлетворяют всем перечисленным выше пяти принципам, однако используют в процессе своего функционирования знания (например, в виде правил или в виде обученной на основе экспериментальных данных нейронной сети) как средство преодоления неопределенности информационной среды. Такие системы принято называть **системами, интеллектуальными «в малом».**

Для реализации представленных на рис. 1.4 функций управления можно воспользоваться структурной схемой интеллектуальной системы управления, приведенной на рис 1.5. В общем случае данная система получает задание от оператора (администратора системы), однако возможен вариант ее автономной работы без вмешательства оператора по заложенному при настройке критерию цели.

Рис. 1.5. Обобщенная структура интеллектуальной системы управления

В состав системы входят следующие модули (подсистемы):

- ***«Диалоговое общение»*** обеспечивает ввод и обработку в интерактивном режиме задания (входной командой информации), а **также** обратную выдачу подтверждений о понимании задания или запросов на его уточнение;

-*«Формирование цели»* - обеспечивает анализ возможности выполнения задания при существующих на данных момент ресурсах системы и состоянии ее компонентов, при решении о невозможности выполнения задания формируется ответ с объяснениями отказа и предложением коррекции задания;

- *«База знаний»* (БЗ) - содержит формализованное в рамках выбранного метода и языка представления знаний описание объекта, его среды и правила , необходимые для выполнения поставленного задания;

- *«Извлечение знаний»* - обеспечивает формирование знаний о внешней среде путем интеграции полученной внешней информации и корректирующей (уточняющей) информации от оператора;

- *«Обучение и самообучение»* - обеспечивает накопление дополнительных знаний о проблеме в режиме «с учителем» и «без учителя» (т.е. автономно);

- *«Вывод на знаниях / формирование плана действий»* - осуществляет обработку цели и знаний о среде и проблеме для прогнозирования и формирования управляющих воздействий, подаваемых на исполнительные механизмы (подсистемы) объекта;
- *«Обработка внешней и внутренней информации»* - производит оценку изменения текущего состояния среды и объекта управления на основании информации, полученной от различных устройств (сенсоров), связывающих систему с внешней средой (внешние источники информации), и от датчиков состояния объекта системы;

- *«Контроль и диагностика»* - обрабатывает **полученную** внутреннюю информацию об изменениях состояния объекта и системы с целью выработки контрольной информации, позволяющей анализировать возможность выполнения задания, поставленного перед системой

В основе функционирования интеллектуальной системы (рис. 1.5) используется идея ситуационного управления , суть которого заключается в выборе управленческих решений с учетом сложившейся ситуации из некоторого набора допустимых (типовых , стандартных) управляющих воздействий. Под текущей ситуацией (С) при этом понимается совокупность текущего состояния объекта (вектор состояния X) и его внешней среды (вектор возмущений F) :

$$C=<X,F>. \qquad (1.1)$$

Полная ситуация (S) включает в себя, помимо текущей ситуации С, также цель управления G:

$$S =< C,G >. \quad (1.2)$$

В частном случае, цель управления G может быть представлена в виде некоторой *целевой ситуации* C_g, к которой должна быть приведена имеющаяся текущая ситуация:

$$S =< C,G_g >. \qquad (1.3)$$

Полагая, что текущая ситуация С принадлежит некоторому классу *Q'*а целевая (заданная) ситуация C_g - классу *Q*", будем искать такое

управление (вектор управляющих воздействий U), которое принадлежит множеству допустимых управлений Ω_U и

обеспечивает требуемое преобразование одного класса ситуаций в другой

$$\mathbf{C} \in Q' \xrightarrow{U \in \Omega_U} \mathbf{G}_g \in Q''. \qquad (1.4)$$

Таким образом, ситуационное управление выступает как отображение

$$(Q', Q'') \to \mathbf{U} \in \Omega_u, \qquad (1.5)$$

сопоставляющее паре «текущая ситуация - целевая ситуация» требуемый результат — управление U. Другими словами, проблема выбора управляющих воздействий сводится к адекватной оценке состояния объекта и среды (что не всегда легко сделать в условиях факторов неопределенности), отнесению соответствующей текущей ситуации к одному из типовых классов и выбору такого управления (из определенного набора альтернатив), которое приводит к достижению поставленной цели управления (целевой ситуации). Очевидно, что перечисленные выше положения, касающиеся общих принципов построения интеллектуальных систем, имеют универсальный характер и в полной мере относятся к таким сложным объектам управления, какими являются объекты защиты информации. Вместе с тем на пути создания интеллектуальных систем защиты информации пока имеется много нерешенных проблем, характерных для данной предметной области (существует даже официально утвержденный *INFOSEC*

Как отмечается в литературах (учитывая важность высказанных соображений, процитируем их практически полностью), «... основные недостатки традиционных СЗИ определяются сложившимися жесткими принципами построения архитектуры и заключаются в практической неспособности противодействовать современному информационному оружию. В современных СЗИ в основном применяются оборонительные или наступательные стратегии защиты, которые предназначены только для блокировки всех известных и наиболее опасных потенциальных способов специальных программно-технических воздействий (СПТВ), осуществляемых противником для нанесения ущерба информационным ресурсам автоматизированной системы (АС). Эти стратегии являются изначально проигрышными, так как не позволяют СЗИ АС успешно противодействовать всем потенциальным способам СПТВ, следовательно, для решения этой проблемы необходимо использовать в СЗИ АС исключительно упреждающую стратегию защиты, в основе которой должна быть способность полной адаптации к любым изменениям условий функционирования АС, вызванным применением противником информационного оружия.

Постоянная разработка новых методов и средств СПТВ и наблюдаемая в последнее время тенденция к постоянному росту количества случаев успешной реализации СПТВ требуют принципиально новых подходов к обеспечению безопасности в АС.

Этим обусловлена актуальность создания теории интеллектуального обеспечения безопасности информации АС. В рамках создания теории необходимо комплексное решение ряда функциональных научных проблем, направленных на исследование и разработку новых теоретических моделей и методов для создания на их основе нового поколения интеллектуальных отечественных СЗИ:

- разработка аксиоматической модели угроз безопасности информации;
- создание математической теории идентификации СПТВ на АС;
- создание новых математических моделей систем разграничения доступа, соответствующих информационным процессам в АС;
- создание методологии построения адаптивных СЗИ АС;
- создание методологии построения систем поддержки принятия решений при обеспечении ЗИ в АС;
- разработка замкнутой системы метрологических критериев оценивания защищенности информации АС;
- создание общей теории информационных рисков;
- создание методологии обеспечения собственной безопасности

СЗИ АС.

Решение указанных фундаментальных научных проблем позволит создавать новые интеллектуальные СЗИ, основным преимуществом которых будет способность предотвращения, обнаружения и нейтрализации, использования методов и средств СПТВ, имеющих априорную параметрическую и сигнальную неопределенность.

Основные требования, которым должна удовлетворять перспективная интеллектуальная СЗИ:

- способность обнаруживать априорно неизвестные СПТВ;

-автоматизированная поддержка принятия решений о противодействии СПТВ;

-способность автоматического оценивания изменения уровня защищенности АС от СПТВ при изменении условий функционирования;

-автоматизированная поддержка принятия решений о перераспределении ресурсов СЗИ АС;

-автоматическое изменение своих свойств и параметров в зависимости от изменения условий среды функционирования, на основе накопления и использования информации о ней;

-способность к дезинформации нападающей стороны об истинных свойствах и параметрах АС;

Исходя из вышеизложенного, архитектура перспективной интеллектуальной СЗИ АС должна включать в себя следующие функциональные компоненты:

- подсистему обнаружения СПТВ;
- подсистему накопления данных;
- подсистему анализа защищенности;
- подсистему адаптации СЗИ;
- подсистему активного противодействия СПТВ» .

Данной тематике в последнее время уделяется большое внимание в специальной литературе. Так, вопросам интеллектуального противодействия информационному нападению в корпоративных информационно-вычислительных сетях специалистами предлагается использовать для этих целей аппарат обучаемых *M*-сетей, генетические алгоритмы оптимизации, концепцию «искусственной жизни». Общая концепция построения модели адаптивной системы защиты информации, реализуемой на основе биосистемной аналогии с использованием интеллектуальных механизмов нейронных сетей и нечеткой логики. Конструктивные подходы, связанные с построением моделей комплексной оценки угроз безопасности информации, анализом информационных рисков, построением систем обнаружения атак и систем поддержки принятия решений по управлению ЗИ с использованием методов искусственного интеллекта, рассматриваются в работах ведущих ученных в области ИБ и др. Разработке методов и алгоритмов управления защитой информации в корпоративных информационных системах с использованием интеллектуальных технологий посвящена докторская диссертация И.В Машкиной.

Вместе с тем в силу широты и многоплановости проблемы создания интеллектуальных СЗИ, ограничимся рассмотрением лишь отдельных частных аспектов (задач) в рамках решения этой проблемы, связанных с построением ряда ключевых функциональных подсистем СЗИ с применением методов искусственного интеллекта.

Вопросы:

- **Что понимается под интеллектуализацией систем защиты информации?**
- **Перечислите основные принципы структурной организации интеллектуальной системы.**
- **Каковы основные направления развития интеллектуальных систем защиты информации?**
- **Каким основным требованиям должна удовлетворять интеллектуальная система защиты информации?**

Литература:

- **Васильев В.И. Интеллектуальные системы защиты информации. 2017 г.**
- **Цирлов В.Л. «Основы информационной безопасности информационных систем», издательство «Феникс», 2008 г., 173 с.**
- **Петров В.П., Петров С.В. «Информационная безопасность человека и общества», издательство «Энас», 2007 г., 336 с.**
- **Скотт Бармен «Разработка правил информационной безопасности», издательство «Вильямс», 2002 г., 208 с.**