Интеллектуализация систем защиты информации

Под **интеллектуализацией СЗИ** понимается повышение ее интеллектуальных возможностей с целью обеспечения высокого уровня её автономности, адаптивности и надежности в условиях неопределенности:

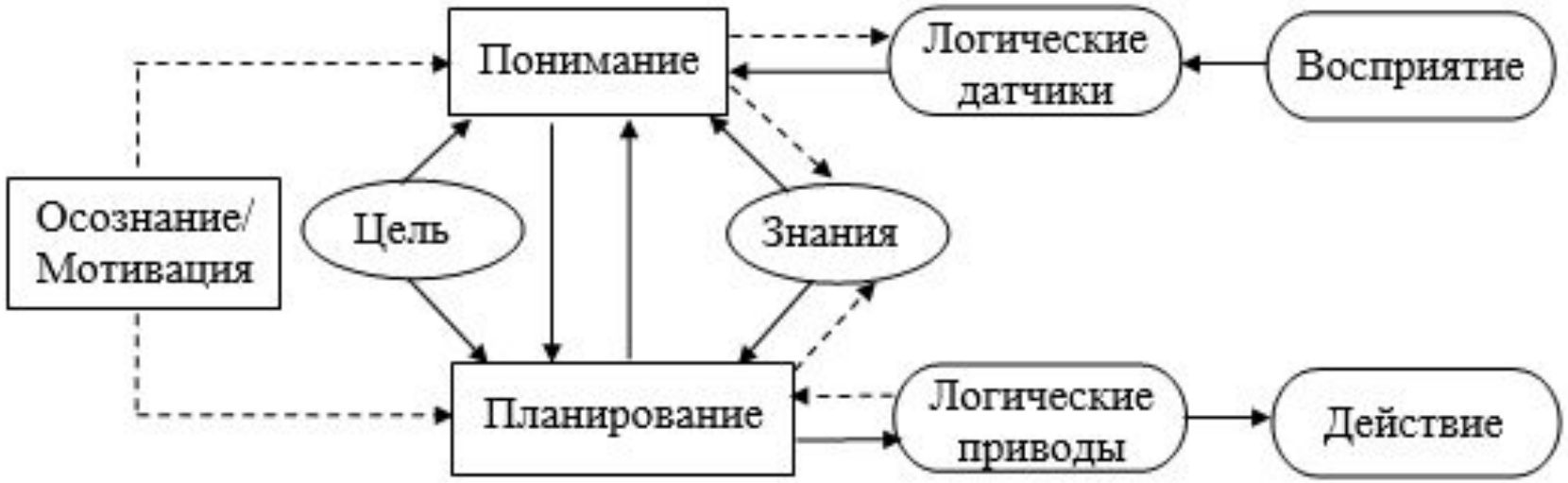
- передача компьютеру максимально возможного количества функций по сбору, обработке информации и принятию решений, чтобы помочь пользователям и администраторам системы получить более объективную оценку событий, происходящих на объекте (в системе), и принять правильные и своевременные решения;
- в качестве средства борьбы с неопределенностью выступают методы и технологии искусственного интеллекта.

Интеллектуализация систем защиты информации

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.

Структура интеллектуальной системы



Результат решения задачи (действие) = анализ и обработка поступающей входной информации + (восприятие) с помощью системы правил (знаний)

«Действие» = «анализ» на основе «знаний»

Интеллектуализация систем защиты информации

- Интеллектуальная система формирует результат решения задачи (***действие***) на основе анализа и обработки поступающей входной информации (***восприятие***) с помощью определенной системы правил (***знаний***).
- ***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*** (желаемым состоянием), производится ***планирование*** − принятие решения о выполнении действий для уменьшения рассогласования при заданных ограничениях.
- Блок ***осознания/мотивации*** выполняет функцию слежения за пониманием и планированием.

Интеллектуализация систем защиты информации

Если система не может понять полученные с помощью логических датчиков данные, то **осознание/мотивация** может приспособить (изменить) знания и сделать полученные данные более доступными для понимания.

Два **режима работы** интеллектуальной системы:

- режим решения поставленной задачи
- режим обучения/самообучения.

Интеллектуализация систем защиты информации

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».

Интеллектуализация систем защиты информации

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».

Интеллектуализация систем защиты информации

- 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.
- Об интеллектуальных системах говорят как о **системах, основанных на знаниях** (*Knowledge-Based Systems*).

Принципы структурной организации ИС

Для обеспечения свойства интеллектуальности системы необходимо придерживаться следующих **принципов её структурной организации**:

- наличие информационного взаимодействия с внешним миром и использование информационных каналов связи;
- открытость системы для повышения интеллектуальности и совершенствования поведения;
- наличие механизмов прогноза изменений внешнего мира и собственного поведения системы в динамически меняющемся внешнем мире;
- наличие многоуровневой иерархической структуры, построенной в соответствии с правилом: повышение интеллектуальности и снижение требований к точности моделей по мере повышения ранга иерархии (и наоборот);
- сохраняемость функционирования (возможно, с потерей качества или эффективности) при разрыве связей или потере управляющих воздействий от внешних уровней иерархии в системе.

Принципы структурной организации ИС

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

Система, интеллектуальная «в большом», должна иметь многоуровневую иерархическую структуру:

- исполнительный уровень;
- уровень координации (тактический уровень);
- уровень планирования (стратегический уровень).

Принципы структурной организации ИС

Отличие СЗИ и ИС ЗИ

Интегрированная СЗИ основной упор делает на **применение традиционных методов**, «жестко» запрограммированных алгоритмов или (на верхних уровнях иерархии) участие оператора в процессе принятия решений;

Главной целью является обеспечение согласованной работы всех подсистем, как единого целого, для поддержания заданного уровня защищенности информационной системы (объекта защиты).

Интеллектуальная система главное внимание уделяет достижению поставленных целей ЗИ за счет **повышения эффективности процессов обработки информации и принятия решений** на каждом из уровней управления на основе применения интеллектуальных технологий.

Принципы структурной организации ИС

На практике интеллектуальные системы могут не удовлетворяют всем пяти принципам, но 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.

Системы интеллектуальные «в малом».

Структурная схема интеллектуальной системы управления

Система получает задание от оператора (администратора системы), или работает автономно по заложенному критерию цели.

Структурная схема интеллектуальной системы управления

Структурная схема интеллектуальной системы управления (1)

В состав системы входят следующие модули (подсистемы):

- ***«Диалоговое общение»*** – обеспечивает ввод и обработку в интерактивном режиме задания и обратную выдачу подтверждений о понимании задания или запросов на его уточнение;
- ***«Формирование цели»*** – анализ возможности выполнения задания при существующих ресурсах системы и ее состоянии; при решении о невозможности выполнения задания формируется ответ с объяснениями отказа и предложением коррекции задания;
- ***«База знаний»*** (БЗ) – содержит формализованное описание объекта, его среды и правила, необходимые для выполнения поставленного задания.

Структурная схема интеллектуальной системы управления (2)

В состав системы входят следующие модули (подсистемы):

- ***«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;

Структурная схема интеллектуальной системы управления (3)

В состав системы входят следующие модули (подсистемы):

- ***«Обработка внешней и внутренней информации»*** – оценка изменения текущего состояния среды и объекта управления на основании информации, полученной сенсоров, связывающих систему с внешней, и от датчиков состояния объекта и системы;
- ***«Контроль и диагностика»*** – обрабатывает внутреннюю информацию об изменениях состояния объекта и системы для выработки контрольной информации, позволяющей анализировать возможность выполнения задания.

Интеллектуальная система управления

В основе функционирования интеллектуальной используется идея **ситуационного управления:**

- выбор управленческих решений с учетом сложившейся ситуации из некоторого набора допустимых (типовых, стандартных) управляющих воздействий.

Интеллектуальная система управления

Под *текущей ситуацией* (**C**) понимается совокупность текущего состояния объекта (вектор состояния **X**) и его внешней среды (вектор возмущений **F**):

$$\mathbf{C} = < \mathbf{X}, \mathbf{F} > .$$

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

$$\mathbf{S} = < \mathbf{C}, \mathbf{G} > .$$

Интеллектуальная система управления

Цель управления **G** может быть представлена в виде *целевой ситуации* $\mathbf{C}_g$, к которой должна быть приведена имеющаяся текущая ситуация:

$$\mathbf{S} = < \mathbf{C}, \mathbf{G}_g > .$$

Интеллектуальная система управления

Дано: текущая ситуация ***C*** принадлежит некоторому классу ***Q'***, а целевая ситуация C_g – классу **Q''**.

Найти: вектор управляющих воздействий **U**, который принадлежит множеству допустимых управлений Ω_U и обеспечивает требуемое преобразование одного класса ситуации в другой:

$$\mathbf{C} \in Q' \xrightarrow{\mathbf{U} \in \Omega_u} \mathbf{G}_g \in Q''.$$

ситуационное управление выступает как отображение

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

Интеллектуальная система ЗИ

[Бородакий, 2005]:

- Основные недостатки традиционных СЗИ = жесткие принципы построения и неспособность противодействовать современному информационному оружию.
- Оборонительные или наступательные стратегии защиты предназначены только для блокировки всех известных и наиболее опасных *способов специальных программно-технических воздействий* (СПТВ).
- Стратегии изначально проигрышные, так как не позволяют успешно противодействовать всем потенциальным способам СПТВ.
- Следовательно, необходимо использовать в СЗИ упреждающую стратегию защиты на основе способности полной адаптации к любым изменениям условий функционирования ИС

Интеллектуальная система ЗИ

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 ИС от СПТВ при изменении условий функционирования;
- автоматизированная поддержка принятия решений о перераспределении ресурсов СЗИ ИС;
- 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 ИС;
- способность к снижению нецелевой нагрузки на комплекс средств автоматизации ИС;
- автоматическое воздействие на ресурсы нападающей стороны (время, вычислительные и коммуникационные ресурсы).

Архитектура перспективной интеллектуальной СЗИ

Архитектура перспективной интеллектуальной СЗИ ИС должна включать в себя следующие функциональные компоненты:

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