Раздел 1.1: «Элементы искусственного интеллекта»

В настоящее время не существует единого определения искусственного интеллекта (ИИ). Формулировки, приведенные в верхней части таблицы, касаются мыслительных процессов и способов рассуждения, а в нижней части таблицы находятся формулировки, касающиеся поведения. В определениях, приведенных слева, успех измеряется в терминах достоверного воспроизведения способностей человека, а формулировки, находящиеся справа, характеризуют конечные достижения с точки зрения принципа рациональности.

Таблица 1 – Системный подход к определению ИИ

Системы, которые думают подобно людям	**Системы, которые думают рационально**
«[Автоматизация] действий, которые мы ассоциируем с человеческим мышлением, т.е. таких действий, как принятие решений, решение задач, обучение...»	«Изучение умственных способностей с помощью вычислительных моделей»
Системы, которые действуют подобно людям	**Системы, которые действуют рационально**
«Наука о том, как научить компьютеры делать то, в чем люди в настоящее время их превосходят»	«Искусственный интеллект... - это наука, посвященная изучению интеллектуального поведения артефактов»

Под системой искусственного интеллекта может пониматься система, способная решать задачи, требующие интеллектуальности от людей, решающих подобные задачи. Такие системы демонстрируют лучшие результаты в ограниченных, хорошо формализуемых предметных областях. Например, программа Deep Blue компании IBM стала первой компьютерной программой, которой удалось победить чемпиона мира в шахматном матче. Однако шахматы являются единственной предметной областью, в которой Deep Blue демонстрирует способности, превосходящие человеческие. Таким

образом, подобным системам не хватает универсальности и гибкости, характерных для естественного интеллекта.

Принцип рациональности был введен Алленом Ньюэллом и заключается в том, что агент выбирает действия, способствующие достижению его целей. Если рассматривать агента с этой точки зрения, то предполагается, что он обладает некоторыми знаниями, целями и совершает действия, способствующие достижению целей, настолько, насколько позволяют его знания.

Аллен Нюэлл и Герберт Саймон, создавшие программу GPS (General Problem Solver — Универсальный решатель задач), стремились не только к тому, чтобы их программа решала поставленные перед ней задачи. Также было важно, чтобы последовательность рассуждений, проводимых программой, соотносилась с рассуждениями людей, решавших подобные задачи.

Утверждение, согласно которому машины, возможно, обладают способностью действовать интеллектуально, философы называют гипотезой слабого **искусственного интеллекта,** а утверждение, что машины действительно мыслят (а не просто имитируют мыслительные процессы), называется гипотезой **сильного искусственного интеллекта.**

Ключевые вопросы философии ИИ — могут ли машины мыслить, обладать сознанием и самосознанием — на данный момент остаются без определенного ответа. Это связано в первую очередь с тем, что механизмы работы человеческого сознания и разума изучены недостаточно хорошо, чтобы проводить убедительные эксперименты с машинами. Эти вопросы в основном являются предметом исследований философов ИИ, например, Дэниела Деннета, Джона Серла и др.

Алан Тьюринг в своей статье «Вычислительные машины и разум» анализировал различные доводы против гипотезы сильного ИИ и предлагал свои способы разрешения этого вопроса. Также он отмечал, что прогресс в области ИИ возможен, даже если пока не найдены ответы на вопросы, поставленные в рамках этой гипотезы.

Гипотеза слабого ИИ предполагает постановку более практического вопроса — создание машин, способных решать задачи, ограниченные какой-либо предметной областью. В связи с тем, что так называемые системы слабого ИИ являются узкоспециализированными, они способны решать достаточно сложные задачи, часто на уровне сопоставимом с человеческими способностями. Вот неполный **список направлений**, в которых могут применяться подобные системы:

- Распознавание речи (голосовой интерфейс, поисковые системы, идентификация пользователя по голосу)

- Машинное зрение (распознавание образов, обработка изображений, распознавание рукописного текста)
- Машинный перевод
- Интеллектуальный анализ данных
- Системы поддержки принятия решений и экспертные системы

Для всех таких систем характерны общие проблемы, связанные с их специализацией. Например, современные системы голосового интерфейса способны распознавать человеческую речь, но несмотря на это часто совершают неожиданные ошибки как в распознавании, так и в интерпретации речи или команд.

На данный момент наиболее распространенной технологией, применяемой для решения задачи распознавания речи, а также в области машинного зрения, являются **искусственные нейронные сети** (ИНС). Но стоит оговориться, что при всей своей популярности ИНС являются только одной технологией из множества, подходящих для решения подобных задач.

Существует множество алгоритмов, применяемых в области машинного зрения. Для примера кратко рассмотрим библиотеку, реализующую алгоритм Mask R-CNN (Region Convolutional Neural Network) [13]. В ней используется **сверточная нейронная сеть**, очень хорошо подходящая для решения задачи распознавания изображений. Упрощенно, алгоритм работы этой библиотеки можно разделить на следующие этапы:

- На основании цветовых и текстурных сходств определяются потенциальные регионы для классификации;
- Из небольших регионов формируются более крупные;
- Отсеиваются неподходящие регионы;
- Выполняется распознавание признаков для конкретных объектов, уточняются их размеры и границы.

В области машинного зрения результаты работы систем ИИ сопоставимы со способностями человека. Однако, например, в задаче машинного перевода демонстрируются более скромные результаты. Одной из причин является неоднозначность естественных языков – в зависимости от контекста смысл слов может изменяться. Для решения этой задачи используются как **статистические методы**, которые не учитывают смысл анализируемого текста, так и **методы, основанные на знаниях.**

Основным приложением методов, основанных на представлении и организации вывода на знаниях, является **создание систем поддержки принятия решений** (СППР) и **экспертных систем** (ЭС). СППР помогают пользователю принимать решения в слабо структурированных предметных

областях. ЭС аккумулируют знания специалистов в предметной области и используются для консультирования менее квалифицированных пользователей. В отличие от ИНС методы, основанные на знаниях, позволяют явно описывать структуру, понятия и закономерности предметной области.

Основным компонентом СППР и ЭС является **база знаний** о предметной области. Для формализации знаний экспертов используются различные **модели представления знаний** [12]. Например, продукционная модель позволяет моделировать рассуждения экспертов с помощью правил вида «если …, то …». Одним из преимуществ СППР и ЭС является возможность объяснить полученные результаты, продемонстрировав последовательность рассуждений. Это позволяет обосновать рекомендации, предлагаемые пользователю.

В заключение стоит заметить, что, хотя современные системы ИИ не обладают так называемым «сильным ИИ», они все же способны решать прикладные задачи. Развитие подходов и технологий, лежащих в основе таких систем, позволяет использовать их для решения все более сложных проблем.

Раздел 2.2: «Анализ данных. Big Data»

Технологии больших данных (Big Data) - это группа технологий и методов производительной обработки структурированных и неструктурированных данных больших объемов в распределенных информационных системах, обеспечивающих организацию качественно новой полезной информации.

Суть технологии больших данных заключается в обработке больших объемов данных. Примерно в 2002 году мы перешли из эпохи аналоговых измерений в эпоху больших цифровых данных или иными словами Big Data.

Источниками Big Data являются технологии, промышленность, экономика и наука.

Сам **термин Big Data** пришел из академической среды и постепенно развился, нашел применение в самых различных **отраслях науки и техники**:

- Системы безопасности
- Ситуационный анализ
- Контроль качества
- Медицина
- Психология
- Педагогика
- Анализ конфликтов

Во всех этих отраслях либо уже применяются, любо в ближайшее время найдут приложения математические методы анализа данных и обработки больших данных.

Какие же **основные качества** присущи большим данным?

- Прежде всего, это **большой объем** – из самого определения очевидно, что большие данные характеризуются большим объемом обрабатываемых данных. Для обработки больших данных используются современные технические средства, поэтому эти характеризуются высокой скоростью обработки.

- Также данные получаются с различного рода сенсоров: и звук, и видео, и различного рода другие сенсоры самого разного вида и характера – поэтому обладают высокой степенью **разнообразия.**

- Также большие данные характеризуются различной степенью **достоверности**. Действительно, технические средства регистрации больших данных обладают высокой степенью достоверности. Например, данные, полученные из социальных сетей, обладают низкой степенью достоверности.

Итак, обратимся к определению.

«Большие данные – новая нефть», т.н. «топливо» для цифровой экономики. Это определение было дано британским математиком, основателем аналитического отдела маркетинга сети супермаркетов Tesco. Впервые он стал утверждать, что большие данные по сути дела являются новой нефтью, служат топливом для современной цифровой экономики. Но, как и от нефти в сыром виде, от цифровых данных в необработанном виде толку мало, их нужно уметь обрабатывать современными математическими методами обработки данных.

Таким образом, мы переходим к вопросу датификации.

Датификация – это вопрос оцифровки характеристик и состояния объекта или процесса на основе обработки больших данных. Слова, местоположение, взаимодействие - все это порождает данные.

Примерами являются уже упомянутая система ГЛОНАСС для локализации объекта на поверхности нашей планеты. Автоматический анализ текста позволяет идентифицировать автора и провести реферирование текстов, т.е. представить информацию в более емком, более сжатом виде.

Это социальные сети. Итак, для обработки больших данных нам необходимо применять математические методы.

Анализ данных:

- область математики и информатики, занимающаяся построением и исследованием наиболее общих математических методов и вычислительных алгоритмов извлечения знаний из экспериментальных данных;

- процесс исследования, фильтрации, преобразования и моделирования данных с целью извлечения полезной информации и принятия решений

Выше дано определение анализа данных. **Суть** анализа данных заключается в приложении современных и классических методов прикладной математики, математической статистики, теории вероятности для обработки таких данных и для принятия решений.

Основные методы интеллектуального анализа данных:

- Методы машинного обучения;
- Методы сжатия данных;
- Методы обработки изображений, видеоаналитика;
- Технологии баз данных;
- Статистический анализ;
- Технологии визуализации;
- Методы распознавания образов;
- Другие технологии и научные дисциплины.

Прежде всего, это методы машинного обучения, методы сжатия информации и представление ее в более компактном, более емком виде, методы видео аналитики, методы обработки изображений. Методы визуализации помогают представить информацию в более наглядном виде. Методы распознавания образов ложатся в основу разработки методов машинного обучения. Методы прогнозирования временных рядов, технологии баз данных и другие технологии – все это служит в качестве аналитики для больших данных.

Итак, современные технические средства и новые математические методы анализа данных позволяют проводить так называемый глубинный анализ данных.

«**Data Mining** – глубинный анализ данных - это совокупность методов обнаружения в данных ранее неизвестных, нетривиальных и скрытых взаимосвязей, практически полезных и доступных интерпретации знаний, необходимых для принятия решений в различных сферах человеческой деятельности». Данное определение Data Mining, введенное известным математиком Ильей Петицким-Шапиро в начале этого века.

Суть «Data Mining» заключается в использовании современных математических методов обработки больших данных с целью поиска новых, ранее неизвестных связей больших данных, и принятие решений на основании новых знаний, полученных с использованием big data.

Какие **математические методы обработки big data, data mining** позволяют обрабатывать такие большие распределенные массивы данных?

Прежде всего, это математические методы:

- классификации;
- кластеризации;
- методы сокращения размерности;
- методы нахождения ассоциации и связей среди данных;
- методы прогнозирования временных рядов, позволяющие определить, например, какой будет цена на акции в следующий день или ближайшие 15 минут;
- методы анализа отклонений (особенно важны для принятия решений в оперативном режиме);
- методы визуализации.

Перейдем к **практическим примерам использования математических методов** обработки больших данных.

- Прежде всего, это классификация и прогнозирование. Такие методы лежат в основе алгоритмов обнаружения дефектов на конвейере, например, с использованием методов технического зрения. Обработка временных рядов

позволяет разработать эффективный алгоритм прогнозирования нагрузки в электроэнергетических системах;

- Средства кластерного анализа лежит в основе алгоритмов сегментирования рынка;

- Математические средства анализа выбросов позволяют обнаруживать мошенничества, например, в мобильном банкинге;

- В тоже время анализ скрытых закономерностей позволяет аналитикам проводить анализ рыночной корзины.

Приведем примеры федеральных и региональных программ, опирающихся на технологии и методы больших данных:

- Прежде всего, это федеральная программа «Умный город», когда пространственно-распределенные данные, получаемые с различного рода сенсоров, поступают в единый аналитический центр для принятия решений.

- Например, части «Умного города» является система «Безопасный город», когда с помощью видеоаналитики можно отследить совершенные преступления и в оперативном режиме, близком к реальному времени, принять розыскные меры и предотвратить то или иное преступление;

- Система «Умный дом» позволяет с помощью современных методов регистрации сигналов аналитическими методами подобрать методы поддержания оптимальной температуры в ваших квартирах;

- Системы «Умные энергосистемы/Energy Internet»;

- «Умные Автотранспортные системы»;

- Интернет вещей.

Все эти программы используют большие данные.

Примером может служить всем очевидное приложение, когда ваш будильник автоматически получает данные из системы контроля трафика, например, предлагаемой компанией «Яндекс», и сигнал, для того чтобы вас разбудить, наступает раньше, и вы не просыпаете, приходите вовремя на работу.

Таким образом, технические средства регистрации больших данных и математические алгоритмы обработки больших объемов данных позволяют повысить производительность труда и лежат в основе современной цифровой экономики.

Раздел 2.3: «Виртуальная и дополненная реальность».

В этом разделе Вы узнаете, что такое виртуальная реальность, о технологиях и методах виртуальной реальности, о программной и аппаратной поддержке виртуальной реальности, об областях применения и о дополненной реальности.

Виртуальная реальность (Virtual reality, VR) - созданный техническими и информационными средствами мир, передаваемый человеку через его ощущения: зрение, слух, осязание и другие.

Также есть и другие определения этого термина, например, под **виртуальной реальностью** понимают контент (например, линейное видео, снятое на панорамную камеру или интерактивные 3D-симуляции), который можно воспроизводить с помощью специальных устройств.

Можно отметить следующие **этапы развития** виртуальной реальности:

- В 1962 году был создан первый прототип мультисенсорного симулятора Sensorama, в котором зритель наблюдал кинопроекцию и ощущал себя внутри этого мира;

- В 1967 году был представлен шлем Сазерленда, который позволял изменять изображения соответственно движениям головы;

- В 1977 году была первая реализация виртуальной реальности на основе компьютерной графики под названием «Aspen Movie Map» . Это программа, которая симулировала прогулку по городу Аспену, давая возможность выбрать между разными способами отображения;

- И в 1989 году был окончательно введён термин «виртуальная реальность» для систем, в которых можно было манипулировать трехмерными объектами.

Можно выделить следующие **технологии виртуальной реальности**:

- Например, панорамные видео, во время воспроизведения которых на компьютере с помощью мыши, а на смартфоне за счет данных гироскопа в любой момент можно изменить точку обзора;

- Так же известна интерактивная виртуальная реальность с использованием VR-контента, который реагирует на действия пользователя, который в свою очередь может управлять им с помощью контроллеров или элементов интерфейса.

Известны следующие **методы виртуальной реальности**:

- Симуляция звуковой панорамы - способность ориентироваться в виртуальном мире с помощью слуха за счет локализации источника звука, что может быть осуществлено с помощью акустических систем;

- **Имитация тактильных** ощущений – с использованием так называемых устройств с обратной связью, когда пользователь получает какое-то воздействие от системы;

- **Управление элементами** виртуальной реальности – с использованием интерфейсов пользователя, наиболее реалистично соответствующих моделируемым, что активно используется в компьютерных играх;

- **И прямое подключение к нервной системе**, в котором данные могут передаваться и непосредственно нервным окончаниям, и даже напрямую в головной мозг посредством нейроинтерфейсов.

Известны как минимум три **варианта программной реализации** виртуальной реальности:

- **Первый** из них - на основе графических движков, когда система полностью моделируется как интерактивный 3D-виртуальный мир в двух проекциях, образующих стереопару. Это может быть создано простыми методами компьютерной графики;

- **Второй** вариант - на основе игровых движков, таких как Unity или Unreal. В этом случае система моделируется, в первую очередь, как интерактивная, и изображение формируется аналогично первому варианту;

- **И третий**, последний тип, это на основе платформ виртуальной реальности, когда система позволяет создавать новые интерфейсы взаимодействия.

Существует и **аппаратная поддержка** виртуальной реальности,

- Например, шлем виртуальной реальности (или HMD-DISPLAY), который в настоящий момент представляет собой очки, содержащие один или несколько дисплеев, на которые выводятся изображения для левого и правого глаза, а также систему трекинга для отслеживания внешних объектов;

- Motion-parallax-3d-дисплеи - формируют у пользователя иллюзию объёмного объекта за счёт вывода на один или несколько дисплеев специально сформированных проекций виртуальных объектов, сгенерированных исходя из информации о положении глаз пользователя. Такие устройства используются в симуляторах и компьютерных играх;

- Также, виртуальный ретинальный монитор – устройство, которое проецируют изображение непосредственно на сетчатку глаза, в результате чего пользователь видит изображение перед собой. Очень ярким примером такого устройства является Google Cardboard, который представляется собой очки-держатель, куда вкладывается обычный смартфон с изображением двух проекций, которые образуют стереопару и человек видит стереоизображение

Это похожий держатель, в который пользователь вкладывает смартфон с изображением двух проекций стереопары и через линзы наблюдает

стереоизображение, которое меняется за счет изменения данных гироскопа смартфона.

Области применения технологии виртуальной реальности.

Ну, в первую очередь, это, конечно, компьютерные игры, в которых она позволяет создать игровое окружение и помогает игроку максимально погрузиться в него

Симуляторы, в которых виртуальная реальность заменяет виртуальными объектами реальные

В образовании она помогает максимально погрузиться в предметную область, так же как и в медицине и психологии, в кино и видео.

А в промышленности виртуальная реальность помогает использовать модели технологических процессов вместо реальных.

В отличие от виртуальной реальности, дополненная реальность (или augmented reality, или AR) больше относится к технологиям взаимодействия человека и машины, то есть к интерфейсам. **Дополненная реальность** - это результат введения в поле восприятия любых сенсорных данных с целью дополнения сведений об окружении и улучшения восприятия информации.

Сферы применения дополненной реальности:

- В образовании – она может быть использована, например, для воссоздания исторических событий или чтения обычных книг в 3D-проекциях;

- В здравоохранении дополненная реальность помогает при проведении операций, диагностики пациентов, предоставляет возможность работать с моделями, а не живыми объектами;

- В военном деле она помогает совершенствовать оборонительные средства, например, на основе камер ночного видения

Ну и наконец**, тренды развития виртуальной и дополненной реальности**, существующие в настоящее время

- В первую очередь это развитие аппаратной составляющей виртуальной и дополненной реальностей – например, имплементирование и улучшение физических и сенсорных ощущений;

- Далее можно отметить использование виртуальной реальности в тренировочных целях, что предоставляет возможность погрузиться в любую ситуацию, которую возможно компьютерным образом симулировать;

- Также можно отметить разработку прототипов и дизайнов, где виртуальная реальность может симулировать и тестировать каждую деталь, процесс или механизм;

- Также сложился тренд использования дополненной реальности в маркетинге, где она позволяет демонстрировать рекламу не только на любой части экрана, в пределе периферийного зрения, но и в 3D пространстве.

Раздел 2.4: «Основные сетевые угрозы и защита данных».

Основополагающими понятиями информационной безопасности (ИБ) являются понятия конфиденциальности, целостности и доступности.

Конфиденциальность – предотвращение несанкционированного доступа к информации.

Целостность – предотвращение, или хотя бы обнаружение, несанкционированного изменения информации.

Важно понимать, разницу между конфиденциальностью и целостностью. Рассмотрим в качестве примера онлайн-банк. Злоумышленник может не иметь возможности получить информацию о счете клиента, однако если он, тем не менее, может произвести несанкционированные манипуляции со счетом клиента, то целостность будет нарушена, даже если злоумышленник не сможет узнать, каков был конечный результат манипуляций.

Относительно недавней проблемой являются атаки на отказ в обслуживании (Denial of Service, DoS). Они направлены на нарушение **доступности** сервиса для пользователей.

Продолжим наш пример. Предположим, пользователь включает свой компьютер, чтобы воспользоваться услугами онлайн-банка. Каким образом компьютер узнает, что пользователь является самим собой, а не злоумышленником? И далее, когда пользователь входит в свой личный кабинет, как онлайн-банк может удостовериться в легитимности пользователя?

Оба этих вопроса подводят нас к такому понятию ИБ как **аутентификация** – проверка принадлежности пользователю предъявленного им идентификатора. На отдельном компьютере аутентификация обычно подразумевает проверку пароля. Однако при аутентификации по сети может возникать множество дополнительных проблем: злоумышленник может мониторить сообщения, передаваемые между клиентом и сервером, перехватывать и модифицировать их, или повторять сообщения клиента в попытке выдать себя за него. Таким образом, при аутентификации посети большую роль играет используемый **протокол** передачи данных, иными словами структура и порядок передаваемых сообщений, и используемые средства шифрования.

После того как пользователь был аутентифицирован в своем личном кабинете, онлайн-банк должен наложить определенные ограничения на его возможные действия. Это относится к понятию **авторизации** – соотнесению аутентифицированного пользователя и доступных ему информационных ресурсов.

Чтобы познакомиться с возможными видами атак на информационные системы, рассмотрим **таксономию Хансмана**. В ней атаки рассматриваются с точки зрения четырех независимых измерений. **Первое** классифицирует сами атаки:

- **Вирусы** – самовоспроизводящиеся программы, проникающие в систему без ведома пользователя, и производящие деструктивные действия

- **Черви** – самовоспроизводящиеся программы, распространяющиеся по сети без вмешательства пользователя

- **Троянские программы** – программа, выполняющая на первый взгляд безобидное действие, но производящая параллельно деструктивные операции

- **Переполнение буфера** – получение доступа к другому процессу путем переполнения границы буфера фиксированного размера

- **Отказ в обслуживании** – атака, направленная на нарушение доступности сервиса для пользователей

- **Сетевые атаки** – направлены на элементы сети или на сеть в целом и использующие различные сетевые протоколы, от сетевого уровня до прикладного

- **Физические атаки** – направлены на нанесение физического ущерба сети или компьютеру

- **Атаки на пароли** – направлены на подбор пароля и обычно характеризуются большим числом неудачных попыток аутентификации за короткий промежуток времени

- **Сбор информации** – атаки, сканирующие сеть в поиске уязвимостей

Второе измерение классифицирует цели атаки. Они могут быть как аппаратными, так и программными. Аппаратными целями могут быть элементы компьютера – жесткие диски, центральный процессор, либо сетевые устройства – коммутаторы, маршрутизаторы.

Третье измерение описывает уязвимости, которые может использовать злоумышленник для совершения атаки. Известные уязвимости классифицируются в базе данных CVE (Common Vulnerabilities and Exposures).

Четвертое измерение описывает основную цель атаки – так называемую полезную нагрузку (payload). Например, распространяющийся по сети червь может нести в качестве «полезной нагрузки» троянскую программу. В таком случае, его целью будет доставка этой троянской программы на атакуемый компьютер.

В качестве примера технологии, обеспечивающей сетевую безопасность, рассмотрим **протокол HTTPS**, широко используемый для безопасной передачи данных по сети. Он действует поверх протокола HTTP,

который является одним из основных протоколов передачи данных в сети, и добавляет к нему уровень шифрования по протоколу SSL, либо TLS. [5]

Протокол HTTPS позволяет убедиться, что данные передаются именно тому серверу, с которым клиент пытается установить соединение. Даже если злоумышленник перехватит все сообщения, передаваемые между клиентом и сервером, в том числе те, в которых они договариваются об используемых ключах шифрования, он не сможет получить доступ к передаваемой информации.

При передаче данных по протоколу HTTPS сначала происходит SSL рукопожатие, в процессе которого устанавливается защищенное соединение, и затем происходит защищенный обмен данными. Для обеспечения безопасности на этапе SSL рукопожатия используется **ассиметричное шифрование** – то есть для шифрования и дешифрования сообщений используются различные ключи. **Открытый ключ** (public key) находится в открытом доступе, **закрытый ключ** (private key) хранится у его владельца.

После того как вся необходимая служебная информация была передана в процессе SSL рукопожатия происходит защищенный обмен данными. На этом этапе используются алгоритмы **симметричного шифрования** – то есть для шифрования и дешифрования передаваемых сообщений используется один и тот же ключ.

Рассмотрим подробнее **процесс SSL рукопожатия**. В нем можно выделить **следующие этапы:**

1. **Приветствие**. Здесь клиент и сервер обмениваются служебной информацией, необходимой для установления соединения – поддерживаемые протоколы шифрования, поддерживаемая версия протокола SSL и т.п.
2. **Обмен SSL сертификатами** – позволяет клиенту убедиться в легитимности сервера.
3. **Обмен ключами шифрования**, которые будут использоваться для защищенной передачи данных. Так как будет использоваться симметричный алгоритм шифрования, то клиенту и серверу необходимо договориться об одном ключе.

Стоит обратить особое внимание на второй этап. Здесь клиент запрашивает у сервера его SSL сертификат, чтобы удостовериться в подлинности этого сервера. В общем случае обмен SSL сертификатами может быть двусторонним, т.е. сервер так же может запросить сертификат клиента. Однако это случается редко, только в приложениях требующих очень высокого уровня безопасности.

На основании чего клиент может доверять SSL сертификату сервера? Во-первых, если он находится в списке сертификатов, которым клиент

доверяет по умолчанию. Такой список хранится в каждом браузере. Это сертификаты **центров сертификации** (certification authority CA). Они могут выдавать SSL сертификаты другим компаниям. При этом они предпринимают необходимые действия, чтобы убедиться в легитимности этих компаний. Выданные сертификаты подписываются **цифровой подписью** центра сертификации, что позволяет браузеру тривиально определить подлинность этого сертификата. Если SSL сертификат был скомпрометирован, центр сертификации отзывает его и браузер перестает доверять серверам, использующим такой сертификат.

Протокол HTTPS позволяет защитить передаваемые по сети данные от различных видов атак. Однако одного этого протокола недостаточно для обеспечения безопасности в сети. Для организации надежной инфраструктуры необходимо учитывать особенности реализации используемых сетевых протоколов, используемых алгоритмов шифрования, механизма контроля доступа и др. Кроме того, важную роль в этом вопросе часто играет человеческий фактор.

Список использованных источников

1. Защита информации. Основные термины и определения: ГОСТ Р 50922-2006. [Электронный ресурс], режим доступа: http://docs.cntd.ru/document/gost-r-50922-2006;
2. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения: ГОСТ Р 51275-2006. [Электронный ресурс], режим доступа: http://docs.cntd.ru/document/gost-r-51275-2006;
3. Dennett D. C. Intentional systems // The Journal of Philosophy. 1971. Vol. 68(4). Pp. 87-106;
4. Hansman S., Hunt R. A taxonomy of network and computer attacks. Computers and Security. 2005. Vol. 24(1). Pp. 31–43.
5. Haykin S. Neural Networks and Learning Machines (3rd Edition). PHIL. 2010. 936 p.
6. Newell A. and Simon H. A. GPS, a program that simulates human thought // Billing H. (Ed.) Lernende Automaten. R. Oldenbourg, Munich. 1961 p. 109-124;
7. Searle J. R. Minds, brains, and programs // Behavioral and Brain Sciences. 1980. Vol. 3. Pp. 417-457;
8. Stamp M. Information Security: Principles and Practice 2nd Edition. Wiley. 2011. 606 p.
9. Turing A. Computing machinery and intelligence // Mind. 1950. Vol. 59. Pp. 433-460.
10. Whitman M.E., Mattord H.J. Principles of Information Security 6th Edition. Cengage Learning. 2017. 656 p.
11. Гаврилова Т.А. Инженерия знаний. Модели и методы: учебное пособие / Т.А. Гаврилова, Д.В. Кудрявцев, Д.И. Муромцев - СПб: Издательство «Лань», 2016. — 324 с.
12. Кинг Б. Эпоха дополненной реальности / Б. Кинг, А. Лайтман, Дж. П. Рангасвами, Э. Ларк; [пер. Г. Агафонов, Е. Фотьянова]. – М.: Издательство «Олимп-Бизнес», 2018. - 526 с.;
13. Люгер Дж.Ф. Искусственный интеллект. Стратегии и методы решения сложных проблем. М.: Вильямс, 2003. — 864 с.
14. Майер-Шенберг В. Большие данные: Революция, которая изменит то, как мы живем, работаем и мыслим / В. Майер-Шенберг, К. Кукьер. – М.: Манн, Иванов и Фербер, 2014. – 240 с.;
15. Носов Н.А. Виртуальная психология / Н.А. Носов. – СПб: Издательство «Аграф», 2001. – 432 с.;
16. Папагианнис Х. Дополненная реальность. Все, что вы хотели узнать о технологии будущего / Х. Папагианнис; [пер. с исп. В.Г. Михайлова]. – М.: Издательство «Эксмо», 2019. - 288 с.;

17. Рассел С. Искусственный интеллект. Современный подход. 2е издание: Пер. с англ. / С. Рассел, П. Норвиг – М.: Издательский дом «Вильямс», 2006. – 1408 с.;
18. Россохин А.В. Личность в измененных состояниях сознания в психоанализе и психотерапии / А.В. Россохин, В.Л. Измагурова. – М.: Издательство «Смысл», 2004. – 544 с.;
19. Таратута Е.Е. Философия виртуальной реальности / Е.Е. Таратута. – СПб: Издательство «СПбГУ», 2007. – 148 с.;
20. Флах П. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных / П. Флах. – М.: Инфра-М, 2017. – 364 с.;
21. Common Vulnerabilities and Exposures. URL: https://cve.mitre.org;
22. [Электронный ресурс], режим доступа: https://github.com/matterport/Mask_RCNN.