Прочитайте текст. Составьте тезисный план текста. /30 б./

Современное общество информационных технологий

Современное общество информационных технологий основано на повседневном использовании компьютерной техники, сетей связи, мобильных средств коммуникации и других технических средств. Ежедневное функционирование государственных структур, банковской, энергетической, транспортной и многих других систем невозможно без надежной работы компьютерной техники и средств коммуникаций. Информационные технологии стали постоянным спутником современного человека не только на рабочем месте, они вошли почти вовсе сферы человеческой жизни.

Распространение новых информационных технологий, в основе которых лежит широкое использование компьютерной техники и средств коммуникаций, оптимизации и автоматизации процессов во всех без исключения сферах жизнедеятельности, привело вместе с этим к нивелированию границ и переплетению национальных экономик и национальных инфраструктур стран мира. Более того, указанные тенденции привели к формированию единого мирового информационного пространства, где каждый может получить доступ к любой информации в любой точке планеты, осуществлять дистанционно управление собственными активами и активами компании, заключать хозяйственные договора с иностранными субъектами хозяйствования без необходимости личного контакта и т.д.

Вместе с этим, информационное пространство стало местом и, в то же время, непосредственно инструментом преступления. Отныне преступление не требует предварительной «обработки клиента» и личного контакта с потенциальной жертвой. Главным инструментом преступника становится лишь компьютер и доступ к информационно-коммуникационным системам, где он с помощью компьютерных вирусов и других противозаконных технических средств получает доступ к базам данных, банковским счетам, автоматизированным системам управления.

Так, кражи данных платежных карт (банковских счетов) или данных доступа к системе Интернет-банкинга с целью завладения средствами клиентов банка, кража персональных данных и коммерческой информации из частных компьютеров или серверов, умышленное повреждение информационных систем или средств коммуникаций с целью создания убытков компаниям –это далеко не полный перечень подобных угроз, связанных с бурным развитием современных информационных технологий. Все это приводит к появлению такого понятия как киберпреступность.

Понимание киберпреступности: явление, задачи и законодательный ответ. – Сектор развития электросвязи. ITU, 2014. – 394 c.

№1 21.04.2020 20:12:04

2

Прочитайте текст. Составьте назывной план текста. /30 б./

Искусственный интеллект и его применение

Искусственный интеллект обычно присваивают свойству электронной вычислительной машины реагировать на информацию, которая поступает через её входные устройства, почти так же, как и среагировал бы человек в тех же условиях. Значит машина так же, как и человек воспринимает образы и ситуации, принимает те же решения. В идеале ЭВМ должна выдавать ту же эмоциональную окраску мышления и поведения, как и у человека.

Некоторые думают, что искусственный интеллект (ИИ)это некая программа, основанная на нейронных связях или суперкомпьютер моделирующий поведение человека. Рассмотрим, что такое на самом деле искусственный интеллект, где он используется и где впервые он применился.

Начнем с того, что ИИ – это целое научное направление. Она занимается разработкой интеллектуальных машин и особенно интеллектуальных компьютерных программ, направленных на то, чтобы понять человеческий интеллект. При этом используемые методы не обязаны быть биологически правдоподобны. Но проблема состоит в том, что неизвестно какие вычислительные процедуры люди хотят называть интеллектуальным. А так как люди понимают только некоторые механизмы интеллекта, то под интеллектом в пределах этой науки люди понимают только вычислительную часть способности достигнуть целей в мире. Различные виды и степени интеллекта существуют у людей, многих животных и некоторых машин.

При этом как видно такое определение интеллекта не связанно с пониманием интеллекта у человека –это разные вещи. Более того эта наука лишь иногда моделирует человеческий интеллект, т.к. с одной стороны, можно изучить кое-что о том, как заставить машины решить проблемы, наблюдая других людей, а с другой стороны, большинство работ в ИИ вовлекают изучение проблем, которые требуется решать человечеству в промышленном и технологическом смысле.

И.А.Бессмертный. Искусственный интеллект– СПб: СПбГУИТМО, 2010. – 132с.

№1 21.04.2020 20:12:04

3

Прочитайте текст. Составьте вопросный план текста. /30 б./

Кибербезопасность промышленной автоматизации

Киберугрозы – явление не новое, но за последнее десятилетие значимость связанных с ними рисков многократно возросла. Дело в том, что раньше автоматизированные системы управления технологическими процессами (АСУ ТП) были физически отделены от локальных вычислительных сетей и Интернета. В современном мире требования к АСУ ТП изменились: они больше не могут оставаться изолированными от внешнего мира. Также важно отметить возрастающую роль решений автоматизации в рамках концепции промышленного «Интернета вещей». Эта тенденция заставляет абсолютно по-новому взглянуть на проблему обеспечения кибернетической безопасности в промышленной среде.

Мотивы кибератак многообразны: это получение финансовой выгоды, желание нанести ущерб конкурентам, оказать политическое давление. Порой атаки совершаются по личным мотивам недовольными сотрудниками или подрядчиками. Вне зависимости от причин ущерб от несанкционированного вторжения в АСУ ТП оказывается очень весомым. Это не только внеплановые остановки производства и поломки оборудования, но и серьезные репутационные потери, утечка конфиденциальной информации, угроза жизни и здоровью людей, рост риска аварий и даже техногенных катастроф.

На сегодня один из ключевых факторов уязвимости — общая низкая культура процессов обеспечения кибербезопасности. На многих предприятиях не проводится оценка ключевых рисков и не обеспечивается безопасное управление операциями, включая базовое управление паролями. Отсутствует комплексный аудит, не гарантируется согласованное и эффективное соблюдение поли-тик безопасности, а также недооцениваются доступные инструменты контроля и обнаружения угроз. Даже в современном мире весьма распространенными проблемами остаются недостаточный контроль физического доступа на территорию и халатное отношение к процедурам авторизации и аутентификации при входе в корпоративные и промышленные сети (к примеру, слишком легкие, редко изменяемые пароли).

НОВИКОВ Д.А. Кибернетика: Навигатор. История кибернетики, современное состояние, перспективы развития. – М.: ЛЕНАНД, 2016. – 160 с. (Серия «Умное управление»)

№1 21.04.2020 20:12:04

4

Прочитайте текст. Составьте назывной план текста. /30 б./

Искусственный интеллект

При возникновении научного направления “Искусственный интеллект” в 1955 г. на фоне бурного начального развития вычислительной техники предполагалось, что программное решение так называемых интеллектуальных, чаще всего прикладных задач даст возможность сформулировать некие обобщения и построить универсальный машинный интеллект, или, что то же самое, универсальное машинное мышление. Основатели направления прогнозировали относительно короткие сроки – максимум в пределах 20го века. Однако, научное направление, которое можно назвать Алгоритмический искусственный интеллект, не создало пока еще ничего похожего на активное творческое человеческое мышление.

Так не стали интеллектуальным и роботы. Они используются в программируемых технологических операциях, например таких, как покраска автомобиля, либо как игрушки. Их обучение и поведение, как и 40 лет назад, не идет дальше схемы стимул-реакция или динамический стереотип. Алгоритмы принятия решения в этих устройствах просты. Восприятие среды формально ограничено. Проблема анализа зрительных 3х-мерных сцен еще очень далека от эффективного решения. Прогресс основывается не на понимании и реализации функции мышления, а фактически определяется только увеличивающейся мощностью вычислительных средств.

То же самое относится и ко многим другим задачам. В частности, сейчас машины прекрасно играют в шахматы. Практический уровень игры машины сопоставим с уровнем игры чемпиона мира. Машина решает эту задачу за счет мощных вычислительных возможностей в основном перебором и сравнением позиций с использованием как формальных, так и эвристических правил оценки.

Можно сказать, что направление работ “Искусственный интеллект” остается по сей день в основном прикладным направлением, ориентированным на формальное решение сложных “информационных” задач и опирающемся на все увеличивающуюся мощность вычислительных средств. Что касается понимания и моделирования мышления, то алгоритмический искусственный интеллект является очень слабым эмпирическим направлением исследований этой проблемы, объединяющим под общим названием весьма разнообразные разрозненные работы. Принципиального теоретического и практического прогресса не произойдет, пока это направление не станет ориентироваться на какие-то целостные теории работы мозга и пока не будет поставлен и сформулирован хотя бы гипотетический ответ на вопрос: что такое мышление и как оно работает? К сожалению, обнадеживающих перспектив этого в рамках направления “Алгоритмический искусственный интеллект” в настоящее время не просматривается.

Воробьев Е. И., Китов А. И. Медицинская кибернетика. – М.: Радио и связь, 1983. – 240 с.

№1 21.04.2020 20:12:04

5

Прочитайте текст. Составьте тезисный план текста. /30 б./

Актуальность проблемы “риск создания машинного интеллекта”

Сейчас в прессе и научно-популярных статьях часто обсуждается проблема глобальных рисков, с которыми может столкнуться человечество. Одним из этих рисков называется искусственный интеллект. Предполагается, что “Большой искусственный интеллект” превзойдет по своему уровню интеллект естественный и сможет сам себя улучшать. Прогнозируются довольно близкие сроки. Например, 2030 год, но не дальше 2050 года. Все предположения о близких (постоянно отодвигающихся) сроках строятся со ссылкой наякобы имеющиеся успехи и производные развития алгоритмического (программного) искусственного интеллекта, распознавания образов и формальных нейронных сетей.

Обсуждается, каким будет искусственный интеллект по отношению к человеку – дружественным или не дружественным. В частности, предполагается, что машины с таким интеллектом могут вступить в конкуренцию и борьбу с человечеством. Предполагается, что результат борьбы “Большого искусственного интеллекта” с человеком может быть не в пользу человека.

Существует международное общественное “Трансгумманитарное движение”, одной из главных целей которого является подготовка к появлению Большого искусственного интеллекта и призыв к принятию мер, направленных на то, чтобы машинный интеллект был дружественным.

Искусственный интеллект сам по себе не будет ни дружественным, ни недружественным. Он будет пассивным. Таким же пассивным, как компьютерная шахматная программа, выигрывающая у чемпиона мира, но не осознающая это и не стремящаяся к этому.

Кроме того, разрозненные результаты, получаемые в направлении работ, называемом “Искусственный интеллект”, включая распознавание образов и формальные нейронные сети, активного мышления не образуют и к полноценному машинному мышлению не ведут. Никаких конструктивных наметок создания Большого искусственного интеллекта в настоящее время не существует. Нет теории работы мозга в процессе мышления и в физиологии. Из всего этого можно сделать вывод, что никакая “точка сингулярности” на кривой развития искусственного интеллекта в районе 2050 года не предвидится.

Воробьев Е. И., Китов А. И. Медицинская кибернетика. – М.: Радио и связь, 1983. – 240 с.

№1 21.04.2020 20:12:04

6

Прочитайте текст. Составьте вопросный план текста. /30 б./

Бионика

Бионика инициировалась кибернетикой.Если одной из основных идей кибернетики Винера была идея попытаться понять работу живыхсистем управления с использованием знаний о принципах автоматического управления, реализуемых в технических системах, то бионика предполагала реализацию противоположной схемы. Общая цель бионики формулировалась как перенос в технику "изобретений" природы.

Одной из наиболее важных задач бионики считалось использование в вычислительной технике знаний из области нейрофизиологии мозга. Однако достаточно быстро выяснилось, что переносить из нейрофизиологии в вычислительную технику нечего, при этом не только потому, что физиология не располагает достаточной конструктивной и целостной информацией о работе мозга, но и попросту потому, что эта информация вычислительной технике не нужна. Современная вычислительная машина на мозг не похожа.Еще раз подчеркнем, что устройство и принципы работы современной вычислительной машины не имеют ничего общего с устройством и принципами работы мозга.

Кибернетика и бионика замышлялись как междисциплинарные дисциплины. Однако, продуктивное взаимодействие между физиологами и инженерами не получилось. Совместные исследования в основном остались лозунгом. Тем не менее,безусловно,очень полезнымбыло то,что внимание инженеров и математиковбыло привлечено к проблемам, которые до этого считались исключительно делом психологов и физиологов. Это привело к многочисленным попыткам применения к описанию мозга и мышления,как формальных аналитических средств, так и средств программного или технического моделирования. Теории мышления на этой основе построить не удалось,номногие работыоказалисьполезными дляпродвижения в направленииобщего понимания проблем.

Воробьев Е. И., Китов А. И. Медицинская кибернетика. –М.: Радио исвязь, 1983. –240 с.

№1 21.04.2020 20:12:04

7

Прочитайте текст. Составьте назывной план текста. /30 б./

Основные понятия эвристического программирования

Первым доминирующим направлением в области ИИ былонаправление, обычно обозначаемое термином «эвристическоепрограммирование», в котором была принята метафора, что мышление – это поиск в пространстве решений. Данное направление тесно связано слабиринтной гипотезой мышления в психологии и исследованиямиформализации процесса доказательства теорем в математике.

Математика занимается исследованием формальных (символьных) систем. На основе некоторой системы аксиом, определяющейинтересующий математика класс объектов, далее доказываются различныетеоремы о свойствах этих объектов. Таким образом, из истинныхутверждений дедуктивно выводятся другие истинные утверждения.Однако сам процесс поиска математического доказательства являетсянеформальным, то есть лежит вне самой математики: между формальнымиаксиомами и выведенными из них утверждениями находитсянеформальный человеческий разум. Для ученых было естественнымжелание избавиться от этого неформального компонента, для чего былонеобходимо попытаться строго описать процесс решения математическихпроблем.

В результате этих попыток в середине 1930-х годов было разработаноформальное понятие алгоритма как последовательности операций надсимвольными выражениями. Механическое применение алгоритма,описывающего решение некоторой математической задачи, к цепочкесимволом, задающей условие этой задачи, в результате дает новуюцепочку символов – ответ. Поиск решения – это поиск подходящегоалгоритма.

Интересно отметить, что одной из первых формализаций понятияалгоритма является машина Тьюринга, представляющая собой некотороевоображаемое механическое приспособление, выполняющеепреобразование цепочки символов, записанных в ячейках входной ленты, всоответствии с заложенным в нее набором правил. С одной стороны,современные компьютеры, по сути, воплощают собой концепцию машиныТьюринга. С другой стороны, машина Тьюринга воплощала наиболееобщие аспекты мышления…

Итак, мышление сводилось к решению задач, что представлялось какпоиск в пространстве цепочек допустимых операций. То, чтоэвристическое программирование считалось не просто одним из вопросовИИ, а именноподходом к созданию ИИ в целом, говорит о том, наскольковажной в то время виделась концепция поиска.

И.А.Бессмертный. Искусственныйинтеллект– СПб: СПбГУИТМО, 2010. – 132с.

№1 21.04.2020 20:12:04

8

Прочитайте текст. Составьте тезисный план текста. /30 б./

Риски, связанные с дистанционным обслуживанием

На сегодняшний день банковская система большинства стран предоставляет достаточно широкие возможности дистанционного управления финансовыми ресурсами. Наибольшее распространение получили такие системы дистанционного обслуживания как «клиент-банк», «клиент-Интернет-банк», «телефонный банкинг».

Как правило, прежде чем получить доступ к электронным банковским услугам, от клиентов требуется открыть счета, лично явившись в банк, а также пройти надлежащую проверку. Если личная встреча невозможна, то применяются усиленные меры надлежащей проверки клиентов для снижения повышенного риска. Такие меры могут включать предоставление информации, которая может быть проверена по данным из независимого источника, дополнительная проверка предоставляемых документов, подтверждение организации, которая рекомендует клиента и провела в отношении него такую же надлежащую проверку. Однако банкам не рекомендуется открывать счета для оказания электронных банковских услуг без личного контакта с клиентами.

Дистанционная идентификация делает возможным более широкое использование подставных компаний и физических лиц, которым нет необходимости приходить в банк лично, что затрудняет выявление личностей организаторов и исполнителей киберпреступлений.

В дальнейшем при проведении клиентом операции с использованием удаленного доступа, его идентификация может осуществляться с помощью:

- идентификатора (логина) пользователя, пароля, условной фразы, кода, вопросов и ответов (заранее согласованные или задаваемые в определённом порядке вопросы и ответы);

- применения пользователями ключей, смарт-карт, брелоков и т.д.;

- направление одноразового пароля по СМС;

- электронной цифровой подписи.

Подключение финансовой системы к сети Интернет для осуществления дистанционного обслуживания клиентов предоставляет киберпреступникам широкие возможности несанкционированного вмешательства в работу банковских и других платежных систем.

Наиболее значимыми угрозами для систем ДБО со стороны киберпреступников являются:

- кража или изменение (уничтожение) банковской или персональной информации;

- заражение вредоносным программным обеспечением банковских систем;

- блокирование работы систем ДБО с помощью отправки огромного количества массовых запросов через сеть зараженных компьютеров (бот-сеть).

Понимание киберпреступности: явление, задачи и законодательный ответ. – Сектор развития электросвязи. ITU, 2014. – 394 c.

№1 21.04.2020 20:12:04

9

Прочитайте текст. Составьте вопросный план текста. /30 б./

«Некоторые примеры применения теории информации»

Теория информации применяется при изучении вопросов передачи информации по каналам связи, в частности при разработке способов кодирования передаваемой информации. Кодированием называется представление информации в форме, удобной для передачи (в пространстве или во времени). Обратное преобразование называется декодированием.

Кодер источника (КИ) служит для эффективного (оптимального) кодирования, т.е. для устранения избыточности и снижения среднего числа символов на букву сообщения. Это дает выигрыш во времени передачи или в объеме запоминающего устройства (ЗУ) (если нет помех). При наличии помех это позволяет подготовить (сжать) сообщение для дальнейших преобразований – для помехоустойчивого кодирования, что осуществляется кодером канала (КК), который вводит избыточность в сообщение.

Количество информации, передаваемой за единицу времени по некоторому каналу связи, называется скоростью передачи информации. Информация передается по каналу связи, как уже говорилосьпутемпередачи сигналов. Но канал связи не может быть полностью изолирован от воздействия внешней среды. Посторонние явления, протекающие в каналах связи и искажающие сигналы, получили название шумов или помех.

Итак, передача информации происходит в условиях наличия шумов, искажающих полезные сигналы. Шумы могут быть настолько сильными, что искажается информация содержащаяся в сигналах, а иногда и сигналы становятся для приемника совершенно неразличимыми.

Надежность передачи определяется вероятностью приема неискаженной информации. Весьма важна доказанная в теории информации теорема, гласящая, что с увеличением скорости передачи ее надежность уменьшается и, наоборот, за счет уменьшения скорости передачи можно повысить ее надежность. Простейшим способом повышения надежности передачи информации является многократное повторение передачи одного и того же сообщения. Ясно, что при этом снижается общая скорость передачи информации. Более сложные способы повышения надежности передачи и хранения информации предусматривают включение в состав сообщений дополнительных контрольных символов или применение специальных избыточных кодов.

Воробьев Е. И., Китов А. И. Медицинская кибернетика. –М.: Радио исвязь, 1983. –240 с.

№1 21.04.2020 20:12:04

10

Прочитайте текст. Составьте тезисный план текста. /30 б./

Распознавание образов

К проблематике искусственного интеллекта примыкают работы по распознаванию образов. С самого начала развития кибернетики машинное узнавание сложных объектов и, чаще всего, изображений обычно выбиралось для исследования и моделирования интеллекта и, в частности, таких составляющих мышления, как построение системы обобщенных знаний о среде и использования этих знаний в процессе принятия решений. Восприятие зрительной информации представлялось наиболее удобным для компьютерного моделирования мышления и, в то же время, наиболее практически значимым.

Сразу было очевидно, что для полного решения задачи машинного восприятия необходимо “интеллектуальное” распознавание или распознавание “c пониманием”. В то же время, практическая ориентация работ в области автоматического анализа информации, стремление к технической реализуемости привели к серьезной трансформации проблемы. Оказалось практически почти вынужденным упрощение рассмотрения процесса восприятия путем сведения его к классификации по признакам простых статических объектов, рассматриваемых по отдельности. В результате традиционное распознавание образов, с одной стороны, не решает задачу машинного восприятия сложной внешней информации и, с другой стороны, не является серьезным инструментом для моделирования интеллекта. И тем не менее распознавание образов не только при своем зарождении, но часто и сейчас считается важным шагом в понимании и моделировании мышления.

В основе живого восприятия лежит принцип целостности и управление процессом с понятийного уровня модели среды. Классическое распознавание зрительных образов обычно организуется как последовательный процесс, разворачивающийся снизу-вверх, т.е. от изображения к распознаванию, при отсутствии управления восприятием с верхних понятийных уровней. (То же самое в принципе относится и к распознаванию объектов не зрительной модальности.). Этапу распознавания предшествует этап получения априорного описания входного объекта. Операции выделения элементов этого описания, например, признаков, или структурных элементов, выполняются на изображении локально, части изображения получают независимую интерпретацию, то есть отсутствует целостное восприятие, что, в общем случае, может приводить к ошибкам – рассматриваемый изолированно фрагмент изображения часто можно интерпретировать совершенно по-разному в зависимости от гипотезы восприятия, т.е. от того, какой целостный объект предполагается увидеть.

Воробьев Е. И., Китов А. И. Медицинская кибернетика. –М.: Радио исвязь, 1983. –240 с.

№1 21.04.2020 20:12:04

11

Прочитайте текст. Составьте назывной план текста. /30 б./

История компьютерных вирусов

Теоретические основы создания компьютерных вирусов былизаложены в 40-х годах XX столетия американским ученым Джоном фон Нейманом (John von Neumann), который также известен как автор базовыхпринципов работы современного компьютера. Впервые же термин вирус вотношении компьютерных программ применил Фред Коэн (FredCohen). Это случилось 3 ноября 1983 года на еженедельном семинаре по компьютернойбезопасности в Университете Южной Калифорнии (США), где былпредложен проект по созданию самораспространяющейся программы, которую тут же окрестили вирусом. Для ее отладки потребовалось 8 часовкомпьютерного времени на машине VAX 11/750 под управлением операционной системы Unix и ровно через неделю, 10 ноября состояласьпервая демонстрация. Фредом Коэном порезультатам этих исследованийбыла опубликована работа «ComputerViruses: theoryandexperiments» с подробным описанием проблемы.

Поскольку рассматриваемые вирусы - это по сути компьютерныепрограммы, то об их истории можно говорить только начиная с появлениякомпьютеров, то есть с 1946 года, когда в США была выпущена перваяэлектронно-вычислительная машина (ЭВМ) - ENIAC (Electronic Numerical Integrator And Computer). Однако до появления в 1960 году коммерческих компьютеров, доступ к ЭВМ был сильно ограничен и вирусных инцидентовзафиксировано не было.

Первый известный вирус был написан для компьютера Univac 1108 (конец 1960-х - начало 1970-х годов). Он назывался Pervading Animal и фактически представлял собой игру, написанную с ошибкой - с помощьюнаводящих вопросов программа пыталась определить имя животного,задуманного играющим. Ошибка заключалась в том, что при добавленииновых вопросов модифицированная игра записывалась поверх старой версии плюс копировалась в другие директории. Следовательно через некоторое время диск становился переполненным. Поскольку Pervading Animal не был настоящим вирусом, он не содержал процедуры самораспространения и передавался исключительно через пользователей, желающих по собственнойволе переписать программу.

Макаренко С. И. Информационная безопасность: учебное пособие. - Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.

№1 21.04.2020 20:12:04

12

Прочитайте текст. Составьте вопросный план текста. /30 б./

Нехватка механизмов контроля

Для обеспечения работоспособности всех сетей массовых коммуникаций, от телефонной сети, используемойдля голосовых телефонных звонков, до Интернета, требуются централизованное управление и техническиестандарты. В продолжающихся дискуссиях об управлении Интернетом предполагается, что Интернет не имеетотличий по сравнению с национальной или даже транснациональной инфраструктурой связи. Кроме того,необходимо законодательное регулирование Интернета, и законодатели вместе с органами охраныправопорядка приступили к разработке правовых норм, устанавливающих определенную степеньцентрализованного контроля.

Интернет изначально был разработан как военная сеть, построенная по децентрализованной сетевойархитектуре, которая должна сохранять неизменными и действующими свои основные функции, дажеесли компоненты сети были атакованы. В результате сетевая инфраструктура Интернета устойчива квнешним попыткам управления. Интернет изначально не был предназначен для облегчения уголовногорасследования или предотвращения атак внутри сети.

Сегодня Интернет все шире используется для гражданских служб. При переходе от военной к гражданскойслужбе сущность требований к инструментам управления не изменилась. Поскольку сеть основана на протоколах, разработанных для военных целей, инструменты централизованного управленияотсутствуют, и их нельзя ввести без существенного изменения конфигурации сети. Отсутствиеинструментов контроля делает расследование киберпреступлений весьма затруднительным.

Одним из примеров проблем, возникающих из-за отсутствия инструментов управления являетсяспособность пользователей обходить технологию фильтрации, используя услуги кодированнойанонимной связи. Если поставщик услуг доступа блокирует доступ к определенным веб-сайтам снезаконным содержанием, не могутполучить доступ к этим веб-сайтам. Но блокирование незаконного содержания можно обойти, еслипотребители используют серверы анонимной связи, шифрующие сообщения между ними и центральным сервером. В этом случае поставщики услуг могут оказаться не в состоянии блокировать запросы, поскольку запросы направляются в виде зашифрованных сообщений, которые не могут быть открыты поставщикамиуслуг доступа.

Понимание киберпреступности: явление, задачи и законодательный ответ. – Сектор развития электросвязи. ITU, 2014. – 394 c.

№1 21.04.2020 20:12:04

13

Прочитайте текст. Составьте назывной план текста. /30 б./

Структура области искусственного интеллекта

Термин «искусственный интеллект» используется для обозначения большого направления научных и прикладных исследований. Такоеназвание, закрепившееся за этим направлением, у большинства людейскорее ассоциируется с разумными роботами или мыслящими компьютерами, многочисленные образы которых были созданы в научно-фантастических произведениях. Действительно ли специалисты поискусственному интеллекту ставят перед собой столь амбициозные задачи? Многие из них это отрицают.

Сами исследователи выделяют две основные цели своей работы – этоавтоматизация человеческой деятельности, в особенности тех ее видов,которые традиционно считались интеллектуальными, и (2) созданиекомпьютерных моделей, имитирующих процессы решения человеком техилииных интеллектуальных задач в целях объяснения сущности этихпроцессов.

Еще одной возможной целью, о которой, однако, часто забывают,является создание усилителя интеллекта (УИ). Методология УИ-направления не сильно, но все же отличается от методологии ИИ-направления. Но чтоотличается существеннее – это прогнозируемыесоциальные последствия.

Сразу стоит отметить, что первым двум целям соответствуют и дваразличных подхода в ИИ, которые обычно называются техническим (илиэвристическим) и бионическим. В рамках технического подхода психофизиологическая достоверность моделей мыслительных процессов приносится в жертву эффективности, с которой эти модели решают поставленные перед ними задачи, и интеллектуальность компьютерных программ определяется по тому, насколько хорошие результаты ониполучают по сравнению с человеком. При бионическом подходе, напротив,необходимым считается сходство самих процессов решения некоторойзадачи компьютерной программой и человеком в ущерб качестваконечного результата.

Итак, специалисты по ИИ зачастую ставят перед собой не глобальную цель создания мыслящих машин, а более конкретные задачи поиска автоматического решения некоторых интеллектуально трудных задач либо моделирования отдельных аспектов мышления человека или животных.Тем не менее, свое название научное направление «искусственный интеллект» получило не случайно.

И.А.Бессмертный. Искусственный интеллект– СПб: СПбГУИТМО, 2010. – 132с.

№1 21.04.2020 20:12:04

14

Прочитайте текст. Составьте тезисный план текста. /30 б./

Общие направления противодействия киберпреступности

Чрезвычайно быстрое развитие информационных и компьютерных технологий в последнее время приводит к стремительному развитию киберпреступности, поэтому особую актуальность приобретают вопросы предупреждения и противодействия преступлениям в киберпространстве.

Предупреждения киберпреступности базируется на мероприятиях, направленных на снижение риска совершения таких преступлений и нейтрализацию вредных последствий для общества и частного сектора.

Эффективное противодействие киберпреступлениям должно сочетать комплекс правовых (законодательных), технических, организационных и информационных мероприятий.

Крайне необходима, выработка корректного понятийного аппарата, как первого шага на пути к уголовно-правовой борьбе с киберпреступностью. К определению киберпреступности и киберпреступления нужно подходить тщательно не только потому, что в результате неправильной законодательной формулировки можно получить «мертвую» или плохо применимую на практике норму. В силу специфической природы этого вида преступлений, законодательство о борьбе с ними должно приниматься в соответствии со специальными международными документами (такими, например, как Конвенция Совета Европы о киберпреступности), поскольку эффективное противодействие киберпреступности в границах одной страны, без международного сотрудничества, в настоящее время не представляется возможным.

Необходимо усилить ответственность провайдеров услуг для гарантии того, что они анализируют то, как используются их услуги, а также для обеспечения их мотивации по снижению рисков незаконного использования их услуг в целях совершения преступлений.Важным фактором является также надлежащее отношение к соответствующей компьютерной информации, которая представляет собой экономический интерес для другого субъекта, ограничение доступа к ней, использование лицензированных компьютерных программ и антивирусных софтов для защиты компьютера от незаконного взлома.

Важным является так же усовершенствование нормативно-регулятивной базы для обеспечения информационной безопасности, как на государственном, так и на частном уровне. В частности, необходимо наличие и усовершенствование соответствующей системы информационной безопасности в каждом государственном и частном учреждении. Учреждения должны иметь внутренние правовые акты, регламентирующие вопросы информационной безопасности и предусматривающие ответственность сотрудников за несоблюдение правил компьютерной безопасности.

Макаренко С. И. Информационная безопасность: учебное пособие. - Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.

№1 21.04.2020 20:12:04

15

Прочитайте текст. Составьте назывной план текста. /30 б./

Средства управления ключевой информацией

Пятую группу средств, обеспечивающих повышенный уровень защиты,

образуют средства управления ключевой информацией.

Под ключевой информацией понимается совокупность всехиспользуемых в компьютерной системе или сети криптографическихключей. Безопасность любого криптографического алгоритма определяетсяиспользуемыми криптографическими ключами. В случае ненадежногоуправления ключами злоумышленник может завладеть ключевойинформацией и получить полный доступ ко всей информации вкомпьютерной системе или сети.

Основным классификационнымпризнаком средств управленияключевой информацией является вид функции управления ключами. Различают следующие основные виды функций управления ключами:

1. генерация ключей;

2. хранение ключей;

3. распределение ключей.

Способы генерации ключей различаются для симметричных и асимметричных криптосистем. Для генерации ключей симметричных криптосистем используютсяаппаратные и программные средства генерации случайных чисел. Генерация ключей для асимметричных криптосистем представляетсущественно более сложную задачу в связи с необходимостью полученияключей с определенными математическими свойствами.

Функция хранения ключей предполагает организацию безопасного хранения, учета и удаления ключей. Для обеспечения безопасного храненияи передачи ключей применяют их шифрование с помощью других ключей. Такой подход приводит к концепции иерархии ключей. В иерархию ключейобычно входят главный ключ (мастер-ключ), ключ шифрования ключей иключ шифрования данных. Следует отметить, что генерация и хранениемастер-ключей являются критическими вопросами криптографической защиты.

Макаренко С. И. Информационная безопасность: учебное пособие. - Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.

№1 21.04.2020 20:12:04

16

Прочитайте еще раз текст из 1 задания. Составьте аннотацию этого текста. /30 б./

№2 21.04.2020 20:12:04

17

Прочитайте еще раз текст из 1 задания. Составьте развернутое реферативное описание этого текста. /30 б./

№2 21.04.2020 20:12:04

18

Прочитайте еще раз текст из 1 задания. Составьте аннотацию этого текста. /30 б./

№2 21.04.2020 20:12:04

19

Прочитайте еще раз текст из 1 задания. Составьте развернутое реферативное описание этого текста. /30 б./

№2 21.04.2020 20:12:04

20

Прочитайте еще раз текст из 1 задания. Составьте аннотацию этого текста. /30 б./

№2 21.04.2020 20:12:04

21

Прочитайте еще раз текст из 1 задания. Составьте развернутое реферативное описание этого текста. /30 б./

№2 21.04.2020 20:12:04

22

Прочитайте еще раз текст из 1 задания. Составьте аннотацию этого текста. /30 б./

№2 21.04.2020 20:12:04

23

Прочитайте еще раз текст из 1 задания. Составьте развернутое реферативное описание этого текста. /30 б./

№2 21.04.2020 20:12:04

24

Прочитайте еще раз текст из 1 задания. Составьте аннотацию этого текста. /30 б./

№2 21.04.2020 20:12:04

25

Прочитайте еще раз текст из 1 задания. Составьте развернутое реферативное описание этого текста. /30 б./

№2 21.04.2020 20:12:04

26

Прочитайте еще раз текст из 1 задания. Составьте аннотацию этого текста. /30 б./

№2 21.04.2020 20:12:04

27

Прочитайте еще раз текст из 1 задания. Составьте развернутое реферативное описание этого текста. /30 б./

№2 21.04.2020 20:12:04

28

Прочитайте еще раз текст из 1 задания. Составьте аннотацию этого текста. /30 б./

№2 21.04.2020 20:12:04

29

Прочитайте еще раз текст из 1 задания. Составьте развернутое реферативное описание этого текста. /30 б./

№2 21.04.2020 20:12:04

30

Прочитайте еще раз текст из 1 задания. Составьте аннотацию этого текста. /30 б./

№2 21.04.2020 20:12:04

31

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

32

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

33

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

34

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

35

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

36

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

37

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

38

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

39

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

40

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

42

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

43

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

44

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

45

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

46

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

47

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

48

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

49

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

50

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

51

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

52

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

53

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

54

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

55

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

56

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

57

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

58

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

59

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./

№3 21.04.2020 20:12:04

60

Прочитайте текст из задания 1. Составьте на его основе диалог-расспрос. /40 б./