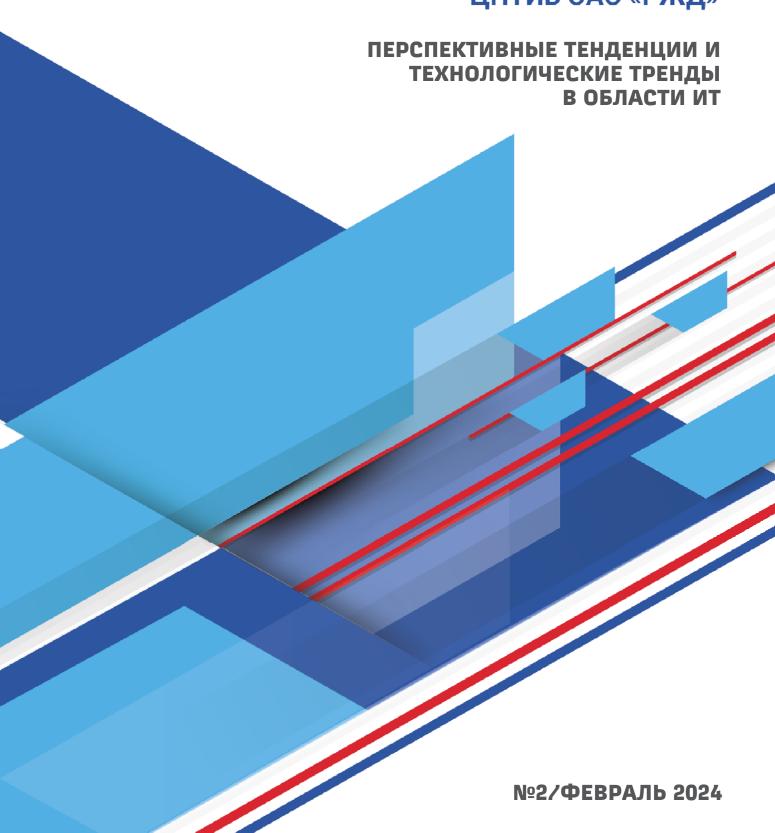


МОНИТОРИНГ

ЦНТИБ ОАО «РЖД»



СОДЕРЖАНИЕ

ЗНАЧИМЫЕ СОБЫТИЯ В ОБЛАСТИ ИТ РОССИИ	4
Путин подписал указ об обновлении стратегии развития ИИ до 2030 года	4
Мишустин озвучил приоритеты развития IT-отрасли в России	5
Как изменится ландшафт киберугроз для промышленных предприятий в 2024 году	7
В России создан консорциум для ІТ-обеспечения исследовательской инфраструктуры	
класса «мегасайенс»	8
МТС внедрила инновационный сервис, который с помощью ИИ предупреждает	
возможные сбои в работе мобильной сети	11
«Росатом» внедрил систему для автоматизации научной деятельности	12
Систему обнаружения препятствий испытали на электропоезде ЭГ2Тв «Иволга»	14
Яндекс запустил нейробраузер	15
В России резко ужесточаются правила импортозамещения ПО. Новшества коснутся	
многих	16
РЖД обновит систему пассажирской навигации на вокзалах	19
Команду ИТ-интегратора Росатома в 2023 году пополнили более 1600 новых ИТ-	
специалистов.	20
«Желдорреммаш» начал подключаться к единой системе управления инженерными	
данными «ТМХ»	20
В России появится новый суперкомпьютер	22
ГК «Солар» получила патент на технологию по оптимизации средств защиты	
информации на основе поведенческих паттернов	23
«Аэроэкспресс» обновил мобильное приложение	24
ЗНАЧИМЫЕ СОБЫТИЯ В ОБЛАСТИ ИТ ЗА РУБЕЖОМ	25
Первая схема сертификации в области кибербезопасности принята в ЕС	25
Цифровой форум ШОС впервые прошел в Казахстане	26
Мошенники использовали дипфейк изображения руководителя компании для получение	КИ
от сотрудника 25 млн долларов (Гонконг)	28
Техника распознавания лиц на основе камеры	30
Компания Duos получила патент на искусственный интеллект (США)	32
Thales Group оснастит поезда лондонского метро системой консультирования	
машинистов	33
Автоматические телефонные обзвоны с генерируемые искусственным интеллектом	
голосом теперь запрещены законом (США)	34
Метрополитен Лондона тестирует инструменты наблюдения с помощью AI в режиме	
реального времени для выявления преступлений	35
Google присоединяется к C2PA, чтобы повысить прозрачность контента, созданного с	
помощью искусственного интеллекта (США)	39
Hitachi Rail испытала пифровую МПП на ВСМ Париж – Лион	40

ОАЭ готовы стать мировым полигоном для испытаний искусственного интеллек	та41
ОАЭ стали мировым лидером по скорости сетей 5G	42
Китай создает собственные стандарты для Web3 и хочет распространить их на ве	сь мир 43

ЗНАЧИМЫЕ СОБЫТИЯ В ОБЛАСТИ ИТ РОССИИ

Путин подписал указ об обновлении стратегии развития ИИ до 2030 года

Согласно указу Президента, в стратегию вносится порядка 40 страниц изменений и дополнений. Обновленная стратегия развития ИИ содержит уточненные принципы развития и использования технологии, соблюдение которых обязательно. К ним относятся прозрачность и объяснимость работы ИИ, а также недискриминационный доступ пользователей к информации об алгоритмах.

В новой стратегии сказано, что «изменение экономической ситуации, односторонние ограничительные меры недружественных иностранных государств и иные изменения рыночной конъюнктуры, которые произошли в 2022–2023 годах, определили новые вызовы для Российской Федерации».

Новым вызовом определено и «ограничение доступа к технологиям искусственного интеллекта в связи с недобросовестной конкуренцией со стороны недружественных иностранных государств».

Обновленная стратегия развития ИИ содержит уточненные принципы развития и использования технологии, соблюдение которых обязательно. К ним относятся прозрачность и объяснимость работы ИИ, а также недискриминационный доступ пользователей к информации об алгоритмах.

В документе сказано, что ежегодный объем оказанных услуг по разработке и реализации решений в области ИИ к 2030 году должен вырасти до 60 млрд рублей, в сравнении с показателем 2022 года в 12 млрд рублей. Помимо этого, планируется увеличить количество выпускников вузов по специальностям, связанным с искусственным интеллектом, с 3 тыс. до 15,5 тыс. человек ежегодно.

«Уровень доверия граждан к технологиям искусственного интеллекта в 2030 году должен вырасти не менее чем до 80% по сравнению с 55% в 2022 году», – говорится в указе.

Кроме того, долю приоритетных отраслей экономики с высокой готовностью к внедрению ИИ намерены нарастить с 12% до 95%.

В 2023 году объем отечественного рынка ИИ достиг 600 млрд рублей, напомнил член комитета Госдумы по информационной политике, информационным технологиям и связи Антон Немкин. «Это позитивный показатель, несмотря на все вызовы, с которыми столкнулась отрасль в 2022 году. Прежде всего, это дефицит высоквалифицированных специалистов. По данным Минцифры, нехватка ИТ-специалистов в целом оценивается в 500—700 тыс. человек. Кроме того, сюда можно отнести существующие

законодательные барьеры, препятствующие развитию технологии. Например, нам нужно ускорить работу над законопроектом по доступу к обезличенным данным, о чем ранее говорил президент», – рассказал депутат.

Обновленная стратегия охватывает все ключевые вызовы, подчеркнул Немкин. «Определение проблемных точек позволит выбрать эффективный инструментарий для их разрешения в дальнейшем. При этом стратегия учитывает как рыночные тенденции, так и запросы граждан страны. Прежде всего, это касается принципа прозрачности и объяснимости работы ИИ. Так, пользователь должен знать не только о том, что перед ним контент, произведённый искусственным интеллектом, но и то, как именно он работает. Фактически это заблаговременное формирование фундамента не только для развития технологии, но и для нивелирования всех рисков, связанных с ней. Подход является правильным в том, что стратегия обновляется в зависимости от происходящих на рынке событий. ИТ-отрасль развивается динамично, и то, что актуально сегодня, завтра таким быть перестанет. Гибкость в этом вопросе как никогда важна», — отметил депутат.

Инструментарий ИИ универсален и может быть задействован практически во всех отраслях экономики страны, подчеркнул депутат. По его словам, это распространяется и на социальную сферу: например, на медицину или образование. «Мы пониманием, что ИИ никогда не сможет заменить человека, но сможет стать для него хорошим подспорьем. Именно поэтому государство заинтересовано в его развитии», – заключил Немкин.

Источник: iksmedia.ru, 19.02.2024

Мишустин озвучил приоритеты развития ІТ-отрасли в России

Приоритетами развития сферы информационных технологий (IT) в России являются запуск мегапроектов технологического суверенитета, подготовка инженеров и внедрение цифровых технологий. На это указал председатель российского правительства Михаил Мишустин на пленарной сессии форума Digital Almaty 2024 в пятницу, 2 февраля текущего года.

«Теперь мы сосредоточились на дальнейшем развитии. <...> Это запуск крупных проектов технологического суверенитета, так называемых мегапроектов, усиление подготовки инженерных команд и внедрение цифровых технологий», – сказал Мишустин.

Премьер-министр РФ отметил, что создание и реализация таких мегапроектов будут способствовать наращиванию производства продукции по

ряду приоритетных направлений, начиная от станкостроения и выпуска авиатехники до фармацевтики и радиоэлектронной промышленности.

Кроме того, он добавил, что для повышения качества подготовки ITспециалистов в России активно строится сеть кампусов мирового уровня, которых в настоящее время уже 17 в стране.

«Сейчас их 17. < ...> В них будут комфортные условия и широкие возможности для получения профессии и ведения исследований. На таких площадках можно готовить и технологические команды стран Евразийского экономического союза», — подчеркнул Мишустин. Всего по поручению президента РФ Владимира Путина к 2030 году должно стать 25 таких кампусов, указал глава российского кабмина.

В ходе выступления Мишустин также отметил, что Россия в настоящий момент входит в тройку мировых лидеров, обладающих серьезными компетенциями в цифровых технологиях. По его словам, страна готова передавать своим партнерам конкретные технологические и платформенные решения, при этом каждая страна сохранит суверенитет данных.

Днем ранее Путин посетил площадку VK на выставке-форуме «Россия» на ВДНХ. Там главе государства рассказали о ряде проектов компании. Так, VK предоставляет бесплатное обучение цифровым профессиям и помогает молодым людям понять, как устроена IT-отрасль и какие профессии в ней есть, а также дает возможность сделать первые шаги в выбранном направлении. За последние два года в них приняли участие свыше 4,5 млн молодых людей.

В середине января Путин поручил правительству разработать и реализовать комплекс мер по увеличению вычислительных мощностей суперкомпьютеров в стране. Кроме того, глава государства поручил кабмину РФ внести изменения в законодательство, которые позволят хозяйствующим субъектам участвовать в экспериментальных правовых режимах в сфере цифровых инноваций.

В конце декабря прошлого года телеканал «Наука» и Институт современных медиа провели опрос, результаты которого показали возросший интерес россиян к развитию информационных технологий. На первое место вышли такие связанные с ІТ темы, как искусственный интеллект (ИИ), нейросети, машинное обучение, а также электроника и нанотехнологии.

Источник: iz.ru, 02.02.2024

Как изменится ландшафт киберугроз для промышленных предприятий в 2024 году

Цифровизация приведет к расширению поверхности атаки, повысится вероятность утечек данных из-за неотлаженных механизмов ответственного раскрытия информации об уязвимостях, вымогатели останутся бичом $N ext{0} 1$, усилится политически мотивированный хактивизм.

Эксперты Kaspersky ICS CERT представили свое видение того, какие тенденции будут наблюдаться в ландшафте киберугроз для промышленных предприятий.

Формирование предпосылок в 2023 году. Стремление к повышению эффективности процессов с помощью цифровизации, в частности использования систем ПоТ и SmartXXX, закономерно ведёт к расширению поверхности атаки. В то же время резкий рост затрат на покупку оборудования и содержание собственной инфраструктуры заставил организации всё больше обращаться к облачным сервисам. Растущая роль государств по всему миру в процессах обеспечения информационной безопасности, помимо очевидного положительного эффекта, привнесла и новые риски, включая повышение вероятности утечек данных из-за неотлаженных механизмов ответственного раскрытия информации об уязвимостях. Эти и многие другие тенденции служат основой для изменений в ландшафте киберугроз, с которыми промышленные предприятия могут столкнуться в 2024 году.

Вымогатели останутся бичом №1 промышленных предприятий в 2024 году. Атаки на крупные организации, поставщиков уникальной продукции и крупные логистические компании чреваты серьёзными экономическими и социальными последствиями. Злоумышленники продолжат атаковать организации, способные выплатить значительный выкуп, что будет приводить к перебоям в производстве и поставках.

Хактивизм

Усилится и будет нести более разрушительные последствия политически мотивированный хактивизм. В дополнение к протестным движениям внутри стран на фоне роста социальной напряжённости (ввиду религиозных и этнических конфликтов и нарастающей экономической нестабильности во многих регионах планеты) получат развитие космополитические протестные движения, поддерживаемые хактивистами, — как следствия внедрения новой социокультурной и макроэкономической повестки. В частности, тема экологии и «зелёных» технологий (возобновляемой энергетики, электромобилей) будет вызывать как поддержку, так и протест эко-хактивистов.

Из «серой зоны» в «тень»

Широкое использование методов «наступательной кибербезопасности» (offensive cybersecurity) для задач сбора данных киберразведки (cyberthreat intelligence) будет иметь как позитивные, так и негативные последствия. С одной стороны, вырастет уровень защищённости организаций, с другой – велик риск нарушений тонкой грани между «серой зоной» и «тёмной стороной» и к услугам «серых» хакеров станут прибегать иногда и в целях, не связанных с обеспечением собственной киберзащиты. В этих случаях будут использоваться коммерческие инструменты и инструменты с открытым исходным кодом, что позволит эффективно маскировать такого рода активность на общем высоком фоне киберкриминальных атак.

Рост числа киберугроз для транспортной и логистической отраслей Продолжающаяся высокими темпами автоматизация и цифровизация логистики и транспорта приведёт к большему сращиванию киберкриминала с традиционным, а также к увеличению вероятности физических последствий случайных заражений.

«Кибербезопасность промышленного сектора постоянно претерпевает значительные изменения: появляются как новые типы атак, так и более изощрённые версии старых. По-прежнему большой проблемой остаются атаки вымогателей, хакеры всё лучше разбираются в том, как атаковать крупные компании с помощью более совершенных методов. Также становятся всё более активными и результативными хактивисты различных толков, что ещё больше усложняет ландшафт киберугроз. Особенно уязвимы к этим изменениям транспортная и логистическая отрасли, ввиду того, что скорость цифровизации высока. Сращивание кибер- и традиционной этих секторах очень преступности представляет собой серьёзную угрозу для глобальных цепочек поставок. Компаниям следует уделять первостепенное внимание и постоянно совершенствовать кибербезопасности методы защиты», комментирует Евгений Гончаров, руководитель Kaspersky ICS CERT.

Источник: iksmedia.ru, 01.02.2024

В России создан консорциум для IT-обеспечения исследовательской инфраструктуры класса «мегасайенс»

Соглашение о создании консорциума для ІТ-обеспечения исследовательской инфраструктуры класса «мегасайенс» подписали президент НИЦ «Курчатовский институт» Михаил Ковальчук, директор Объединенного института ядерных исследований (ОИЯИ) Григорий Трубников и директор Института системного программирования (ИСП) РАН Арутюн Аветисян.

Почетным гостем церемонии, которая состоялась 5 февраля в пресс-центре «Россия сегодня», стал заместитель председателя Правительства РФ Дмитрий Чернышенко.

Сегодня в России интенсивно развивается научная инфраструктура класса мегасайенс — национальная сеть современных больших установок, необходимых для обеспечения прорывных исследований в важнейших направлениях науки, пишет «Россия сегодня».

Развитие исследований мегасайенс приводит к экспоненциальному росту объема экспериментальных данных и темпов их генерации; создаются наборы данных петабайтного масштаба. Впрочем, как подчеркивали мероприятия, потребность в работе с большими данными растет и во многих направлениях В современной науки. частности, Курчатовского института Михаил Ковальчук указал, что сегодня одним из основных «потребителей» IT-ресурсов становится генетика: «У нас бурно технологии расшифровки наследственной информации. создание защищенной системы хранения и обработки этих данных обеспечения необходимое условие российского ДЛЯ технологического суверенитета и биобезопасности».

Для ускоренного развития интенсивных операций с данными проектов мегасайенс и генетических исследований необходимо создать национальную IT-инфраструктуру. Такая инфокоммуникационная сеть обеспечит взаимодействие в этих областях научных и образовательных организаций в России, а в перспективе – и в странах СНГ, ЕАЭС, ШОС и БРИКС.

Для решения задачи объединения инфраструктуры и компетенций в сфере IT-технологий несколько ведущих научных организаций страны выступили с инициативой создания консорциума. Помимо НИЦ «Курчатовский институт» и ОИЯИ в него войдет Институт системного программирования им. В.П. Иванникова РАН.

Как сообщает НИЦ «Курчатовский институт», еще в 2003 году по инициативе центра и Объединенного института ядерных исследований в России был создан Консорциум РДИГ (Российский ГРИД для интенсивных операций с данными – Russian Data Intensive GRID, RDIG) для участия в распределенной обработке данных экспериментов на Большом адронном коллайдере. ОИЯИ также является базовой организацией по созданию и развитию распределенного вычислительного центра стран-участниц Института для мегасайенс-проекта NICA, нейтринной программы (Байкал-GVD, JUNO) и других исследований.

Кроме того, в России работает Национальная исследовательская компьютерная сеть (НИКС), которую развивает и эксплуатирует Курчатовский

институт. Сейчас НИКС объединяет уже более 300 научных организаций и университетов из 37 регионов страны.

РДИГ и НИКС станут базой для создания новой национальной ІТсистемы, которая сможет эффективно обеспечить работу установок мегасайенс, а также Национальной базы генетической информации и биоресурсных центров – ключевых элементов инфраструктуры генетических исследований.

«Сегодня мы объединяем «облачные» разработки Института системного программирования и уникальные возможности, которые есть у Курчатовского института и ОИЯИ. Новая сеть позволит всем нашим ученым иметь доступ к огромным вычислительным мощностям. При этом они смогут участвовать в формировании сервисов, удобных для решения исследовательских задач», – комментирует Михаил Ковальчук.

Он отметил важность развития опережающих компьютерных технологий, способных эффективно работать с технологиями искусственного интеллекта. Эти технологии требуют огромных затрат энергии, и здесь решением может стать, например, разрабатываемый в НИЦ КИ нейроморфный компьютер, потребляющий в 1000 раз меньше энергии. Созданный консорциум может стать важной базой для быстрого достижения таких прорывных результатов.

ГРИД-инфраструктуре «Благодаря И мегасайенс-проекту NICA, Объединенном институте государствами-членами созданным значительном вкладе Российской Федерации, десятки стран мира готовы работать и проводить исследования именно на территории России. Созданный сегодня консорциум – это более чем 30-летние наработки ОИЯИ в области распределенных ГРИД-вычислений как для ЦЕРН, так и для многих европейских и мировых проектов, консолидированные с вычислительными ресурсами Курчатовского института и ряда институтов РАН в рамках Национальной исследовательской компьютерной сети России с сильными технологиями и наработками Института системного программирования в Любой современный научный анализа программных средств. эксперимент требует в первую очередь компьютинга. Я уверен, что наш консорциум будет расширяться», – цитирует пресс-служба ОИЯИ слова директора института Григория Трубникова.

По словам Дмитрия Чернышенко, сегодня в мире не прекращается гонка в области развития искусственного интеллекта и вычислительных мощностей. одна самых перспективных сфер. Производительность ИЗ суперкомпьютеров кратно растёт, примеру, совокупная К мощность вычислительных машин рейтинга топ-500 составляет 7 экзафлопс. Это более чем в четыре раза больше, чем всего пять лет назад. Поэтому крайне важно обеспечить равный доступ российских исследователей к сервисам

вычислительным мощностям. Создаваемый консорциум для IT-обеспечения инфраструктуры «мегасайенс» в том числе позволит решить эту задачу.

Источник: iksmedia.ru, 06.02.2024

МТС внедрила инновационный сервис, который с помощью ИИ предупреждает возможные сбои в работе мобильной сети

Компания МТС внедрила сервис автоматизированного мониторинга качества связи на выделенных сетях Private LTE (pLTE) ряда ведущих российских предприятий. Благодаря ранней диагностике метрик на основе анализа больших данных с помощью искусственного интеллекта система предупреждает возможные сбои в работе мобильной сети, улучшая таким образом, управление производственными процессами в промышленности, сообщает МТС.

Как говорится в сообщении, специалисты компании разработали и внедрили цифровой сервис «Марта» по автоматизированному контролю качества и бесперебойности услуг мобильной связи на выделенных технологических сетях восьми ведущих российских предприятий горнорудной и металлургической отраслей.

Система функционирует во внутренней облачной платформе и связана с базовыми станциями каждого клиента. Благодаря обработке множества параметров — работы сетевых элементов и активности на сети, анализа с использованием ИИ текущей и исторической статистики инцидентов — сервис в автоматическом режиме контролирует работу выделенной сети.

«В случае отклонения от нормы качественных показателей – покрытия, доступности, мобильности и непрерывности – система фиксирует проблему, проводит первичный анализ и передает информацию для дальнейшей обработки экспертам технического блока МТС, предлагая варианты решения ситуации», – отмечается в сообщении.

«Мы планируем масштабировать разработку до стадии коммерческого решения. Для нас крайне важно обеспечивать бесперебойность и высокое качество мобильных услуг в выделенных корпоративных сетях, так как от этого зависит стабильность работы целых производств и безопасность критических технологических процессов на предприятиях наших заказчиков, в число которых входят ведущие предприятия горнорудной, металлургической и энергетической отраслей», — цитируется в сообщении вице-президент по технике МТС Виктор Белов.

Выделенная сеть рLTE предназначена для цифровизации и автоматизации технологических производственных задач, интегрирует И различные беспроводные датчики и ІоТ-устройства, исполнительные механизмы, системы мониторинга и управления с ІТ-инфраструктурой предприятия в единую цифровую экосистему. Изолированность публичных сетей обеспечивает повышенную защищенность, надежность безопасность И производственных и ІТ-процессов.

Источник: ai.gov.ru, 06.02.2024

«Росатом» внедрил систему для автоматизации научной деятельности

В «Росатоме» внедрена и запущена в постоянную эксплуатацию импортозамещеная информационная система для автоматизации и оптимизации процессов научно-технической и инновационной деятельности.

Разрозненные информационные системы, слабо связанные друг с другом и выполняющие отдельные ИТ-функции, изолированные источники данных — так выглядела работа с исследованиями «Росатома» на заре цифровизации научных проектов компании. В 2020 году в корпорации стартовало внедрение проекта «Цифровая наука». В достаточно короткие сроки удалось создать, по сути, научную ERP-систему, позволяющую осуществлять планирование и оптимизацию, обеспечивающие общую модель данных и процессов для научной деятельности.

«Цифровая наука» позволяет повысить качество, прослеживаемость и результативность научной и инновационной деятельности, - рассказала директор по управлению научно-техническими программами и проектами научно-технических директор департамента программ И проектов госкорпорации «Росатом» Наталья Ильина. – В целом цифровизация науки прозрачности способствует научно-технических повышению хода инновационных программ проектов «Росатома», финансируемых И государством. Таким образом, мы пришли от частных информационных систем к мощной корпоративной цифровой системе для управления наукой».

Принципы развития «Цифровой науки» минимизируют ручные процессы, стандартизируют процессы, обеспечивают единство методологии и оптимизируют затраты. Платформа «Комплекс цифровых сервисов (КЦС) «Цифровая наука» реализована на базе импортонезависимого программного обеспечения.

Платформа объединяет в себе 10 сервисов, 25 модулей, три вида баз данных и шесть цифровых инструментов. В декабре 2023 информационная

система была введена в постоянную эксплуатацию и аттестована в соответствии с требованиями безопасности информации ФСТЭК России. Это позволяет «Цифровой науке» обрабатывать, в том числе, персональные данные, информацию для служебного пользования и содержащую коммерческую тайну.

Уже на этапе планирования научных разработок заказчик должен понимать необходимый результат исследований, а также сроки и стоимость его достижения. Поэтому в постановке задач и формировании технических заданий научных проектов «Росатома» участвуют представители науки и бизнеса.

Проводится несколько типов экспертиз: научно-техническая, интеллектуальной собственности, по определению уровня технологической готовности продукта, экономическая экспертиза.

Для этой работы в Росатоме сформирована база экспертов по 12 тематическим научно-техническим деятельностям и 80 продуктовым направлениям. Она включает в себя более тысячи экспертов и полторы тысячи кандидатов в эксперты. Это не только сотрудники госкорпорации, но и ведущие ученые по своим направлениям: представители Российской академии наук, крупнейших вузов, Курчатовского института.

При этом процесс выстроен таким образом, что заказчик не влияет на выбор эксперта, для исключения возможности возникновения конфликта интересов. Процедура проведения экспертизы автоматизирована в «Цифровой науке»: создан сервис подбора экспертов и сформирована коллекция их заключений по видам научно-технических исследований.

«Это важный шаг к автоматизации единой научно-технической работы Росатома и развитию ее в соответствии с целевыми установками на цифровизацию научно-технической экспертизы Минобрнауки РФ и Правительства РФ. Сервис подбора позволяет по ключевым словам, в считанные секунды найти эксперта по всем научно-техническим направлениям Росатома. Все они, включенные в нашу базу, — высококвалифицированные ученые и специалисты, обладающие знаниями и практическими навыками сфер исследований и разработок, формирования тематики НИР, НИОКР, оценки инвестиционных рисков», — поясняет Наталья Ильина.

момент коллекция содержит более полутора данный экспертных заключений. Кроме того, любая экспертная оценка загружается в «Модуль исключения дублирования» «Цифровой науки». Отчет и техническое на оригинальность. задание проверяются Это позволяет дублирование выделения финансирования на одни И те же исследования в отрасли.

В свою очередь, минимизировать трудозатраты при формировании отчетных документов для участников реализации научно-технических и инновационных программ Росатома помогает инструмент «Цифровые шаблоны

документов НИОКР» А для унифицированной оценки уровня технологической готовности результатов научных исследований используют «Калькулятор УТГ».

Источник: rosatom.ru, 09.02.2024

Систему обнаружения препятствий испытали на электропоезде ЭГ2Тв «Иволга»

Компания «ТМХ Интеллектуальные Системы» провела испытание системы обнаружения препятствий на электропоезде ЭГ2Тв «Иволга» на полигоне Москва-Усово. Испытания проходили в режиме подконтрольной поездки.

В основе работы системы — технологии искусственного интеллекта и машинного обучения (рис. 1). Нейросети выявляют рельсовую колею, людей, элементы инфраструктуры, стрелочные переводы, автомобили, подвижной состав и т.д., а алгоритмический аппарат определяет дальности и принимает решения. На испытаниях система визуализировала результаты своей работы два раза в секунду. «В каждом цикле работы системы происходит обнаружение и идентификация объектов в зоне видимости до 600 м во всем поле зрения сенсоров, а также принятие решений, на основе полученных данных»,— сообщается на сайте компании.

Система оборудована лидарами (лазерное радиолокационное оборудование), камерами эмулирующими человеческое зрение (стереопары, на основе этой технологии строится карта глубины кадра), камерами общего плана и ближней зоны, ГНСС-навигатором.

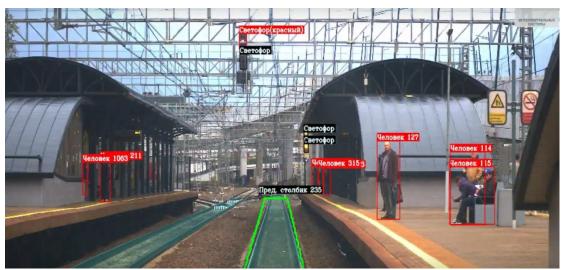


Рис. 1. Как работает система обнаружения препятствий

Данные от сенсоров в режиме реального времени обрабатываются и анализируются специально обученными нейросетевыми алгоритмами, которые подбирают классы и типы объектов. Полученные результаты алгоритмов используются системой для формирования окончательного решения — какие объекты обнаружены, на каком расстоянии, где они находятся относительно поезда и т.д. Исходя из этой информации системы поезда может управлять движением.

Система обнаружения препятствий уже умеет распознавать и классифицировать людей (рабочий путей или обычный прохожий), определять основные объекты железнодорожной инфраструктуры (железнодорожные пути, другие поезда, светофоры и их сигналы, платформы, столбики), определять местоположение поезда и расстояние до ближайших платформ и вокзалов, распознавать автомобили, велосипеды, строить зону габарита — «коридор», в котором разрешено движение поезда и другое.

В дальнейшем эта система будет интегрирована с системами управления поездом. Это позволит автоматически реагировать на препятствия – применять торможение и подавать звуковые сигналы. Также планируется развитие алгоритмов в части точности и стабильности построения зоны габарита, улучшения точности работы стереопары и другое.

Источник: rzddigital.ru, 12.02.2024

Яндекс запустил нейробраузер

Яндекс встроил нейросети нового поколения в Яндекс Браузер. YandexGPT в нейробраузере поможет пользователям писать комментарии, письма, отзывы и другие сообщения. Функция «Помочь с текстом» работает в трёх режимах: «Исправить ошибки», «Сократить» и «Улучшить стиль». Нейросети Яндекс Браузера научились переводить видеоролики с японского и корейского языков на русский и накладывать озвучку. Ранее эта функция была доступна для английского, китайского, французского, испанского, итальянского и немецкого.

Также нейробраузер теперь может кратко пересказывать иноязычные видео с помощью YandexGPT. Он делает это на русском языке и озвучивает результаты суммаризации. Кроме этого, браузер может в режиме реального времени генерировать субтитры для русскоязычных видео, визуально разделяя реплики разных спикеров.

Пользователи нейробраузера Яндекса смогут создавать изображения с помощью нейросети YandexART. Для этого нужно обратиться к Алисе и

текстом или голосом описать то, что хочется увидеть на картинке. Этот режим работы называется «Давай нарисуем».

Непосредственно в Яндекс Браузер втроена ML-модель для проверки сайтов на наличие фишинга. Если она замечает признаки опасности, то запускает комплексную проверку на серверах Яндекса. Всё это занимает менее 0,01 секунды и не влияет на скорость работы. Если сайт действительно опасен, браузер предупредит о рисках и посоветует не переходить на веб-ресурс.

Кроме того, Яндекс Браузер стал значительно быстрее загружаться на компьютерах с устаревшим «железом». Скорость старта в системах, установленных на самые медленные жёсткие диски (HDD), увеличилась более чем в два раза: с 45 до 20 секунд.

Также в нейробраузере доступны:

- сканирование QR-кодов во время воспроизведения видео;
- облачные вкладки и группы вкладок можно открыть вкладку на смартфоне и продолжить работать с ней на ноутбуке и наоборот;
- быстрый перенос настроек и закладок из любого другого браузера в Яндекс Браузер;
- нейросетевые функции Яндекс Браузера активируются с помощью компактных меню – они автоматически появляются рядом с контентом, где их можно применить.

Источник: yandex.ru, 13.02.2024

В России резко ужесточаются правила импортозамещения ПО. Новшества коснутся многих

Власти прорабатывают новые правила перехода на отечественный софт КИИ. объектами Они сторону ужесточения ввиду изменятся приближающейся ПΟ. даты обязательного отказа иностранного Законопроект претерпел множество правок – существует как минимум три его версии.

Тотальный контроль

В России составлен новый законопроект, предоставляющий властям и Центробанку самолично составлять список объектов критической информационной инфраструктуры (КИИ), которые будут обязаны перейти на отечественный софт с 2025 г. Документ существует как минимум в трех редакциях, пишут «Ведомости», ввиду большого количества вносимых в него правок.

Нынешняя российская терминология включает понятие «субъект КИИ» –

госорганизации, юрлица это, В числе прочих, И индивидуальные информационными владеющие предприниматели, системами ИЗ стратегически важных отраслей: транспорта, телекоммуникаций, банковской сферы, атомной энергетики, ТЭК, здравоохранения, науки, металлургии, оборонной, ракетно-космической и химической промышленности. Упомянутые объекты КИИ – это критически важные сети и информационные системы субъектов КИИ.

Запрет на использование иностранного софта на объектах КИИ начнет действовать 1 января 2025 г. Он прописан в указе Президента России Владимира Путина от 31 марта 2022 г. Документ с момента вступления его в силу запрещает субъектам КИИ приобретать иностранное ПО для своих объектов КИИ.

Почти год на разработку

За документом стоит Минцифры – правила и сроки отказа КИИ от иностранного софта с последующим переходом на российский ведомство начало прорабатывать еще весной 2023 г.

Государство хочет самолично указывать бизнесу, что относится к объектам КИИ, а что нет

Нынешняя редакция законопроекта уже рассматривалась в рамках заседания правкомиссии по законопроектной деятельности, состоявшегося 12 февраля 2023 г. Документ к моменту выхода материала располагал положительным отзывом Центробанка и попутно был согласован Минфином, Федеральной службой безопасности России (ФСБ) и Федеральной службой по таможенному и экспортному контролю России (ФСТЭК).

Что именно изменится

По информации издания, текст законопроекта предусматривает корректировку действующего российского закона «О безопасности КИИ». Изменения затронут отдельные системы или объекты в организациях, относящихся к субъектам КИИ.

Пока законопроект не стал законом, субъекты КИИ имеют полное право по собственному усмотрению назначать категории значимости своим объектам КИИ, а некоторые системы и вовсе не относить к таковым, сообщила изданию старший аналитик по информационной безопасности «Лиги цифровой экономики» Елена Камышная.

Именно этой возможности такие компании, фактически, лишатся, если документ будет принят — категории будет раздавать непосредственно государство. Собеседники издания подчеркнули, что по мере появления новых ревизий текста документа прописанные в ней требования становились все более суровыми. Нынешняя, третья по счету редакция, «предполагает более жесткую нормативную базу, ясные требования и невозможность их обойти», утверждает

гендиректор инженерной компании «Уралэнерготел» Алексей Бельский.

От госорганов и Банка России законопроект требует составить списки типовых отраслевых объектов КИИ по классификациям информационных систем и выполняемых ими функций и видов деятельности, после чего согласовать их с ФСТЭК.

Также предложено вести сбор сведений об объектах КИИ на основе предоставленной субъектами КИИ информации. Если компании передадут неполные или ложные сведения об имеющихся в их распоряжении объектах КИИ, то в ответ они могут получить предписание ФСТЭК об устранении нарушений. Такое требование Служба может направить в течение 30 дней, и на его выполнение у компании будет всего лишь 10 дней.

Законопроект не предусматривает штрафы за отказ компании выполнять требование ФСТЭК или срыв сроков внесения достоверной информации об объектах КИИ. Но, напомним, что это уже третья редакция документа — раздел с санкциями вполне может появиться в четвертой, если она будет подготовлена. Также в России существует практика прописывания штрафов и иных видов наказаний не в самом законопроекте, а в подзаконных актах после его принятия. Более того, о возможности появления дополнений в виде этих подзаконных актов говорится непосредственно в тексте самого законопроекта.

Порядок должен быть во всем

Документ требует не только сформировать силами властей каталог типовых объектов КИИ, но и проработать порядок «закупок и использования телекомоборудования и программно-аппаратных комплексов (ПАК) иностранного происхождения», уточняют «Ведомости». Отдельно авторы законопроекта прошлись по российским финансовым организациям — если он будет принят в нынешней редакции, то, по задумке Минцифры, государство и Центробанк получат право принудительно устанавливать и порядок, и сроки перехода таких организаций на «преимущественное использование российского ПО и отечественной радиоэлектронной продукции, в том числе телекомоборудования и ПАК, на принадлежащих им значимых объектах КИИ».

При помощи подзаконных актов к законопроекту в течение полугода после его вступления в силу могут быть добавлены «требования к ПО, радиоэлектронной продукции, используемых на значимых объектах КИИ», реализованные в виде постановления Правительства России. Этими же актами можно будет установить «сроки, порядок перехода и мониторинга субъектов КИИ».

Попытка обосновать необходимость изменений

ИТ-отрасль не встретила новую инициативу властей в штыки. Собеседники издания на отечественном ИТ-рынке отметили, что сейчас субъекты КИИ регулярно и специально снижают степень значимости

имеющихся в их распоряжении объектов КИИ.

По их словам это давняя проблема. Источник издания в российском Правительстве привел в пример систему управления багажом внутри абстрактного аэропорта, которую тот не отнес к объектам КИИ. «При этом мы понимаем, что, когда эта система перестанет работать, произойдет коллапс, что вызовет недовольство пассажиров, — отметил он. — Сейчас собственник рассуждает так: придать объекту статус КИИ — это взять на себя дополнительную ответственность, поэтому пусть лучше объект не имеет такого статуса».

Источник: cnews.ru, 14.02.2024

РЖД обновит систему пассажирской навигации на вокзалах

Компания РЖД планирует в 2024 году обновить систему пассажирской навигации на вокзалах. В результате будет создано единое бесшовное информационное пространство на всем маршруте следования пассажира. Изменения включают продуманную эргономику устройств, упрощенный доступ к интерактивным панелям, централизованное обновление информации на всех динамических табло через единый информационный центр. Об этом сегодня сообщил заместитель генерального директора ОАО «РЖД» Иван Колесников на итоговом заседании правления холдинга.

Планируется, что пилотный проект будет реализован на железнодорожном вокзале в Нижнем Новгороде. Позднее он будет тиражирован на всей сети Российских железных дорог.

Иван Колесников также отметил, что в этом году компания планирует внедрить более 300 улучшений, «которые сделают веб-ресурсы РЖД более функциональными и интуитивно понятными».

В частности, как сообщает пресс-служба РЖД, речь идет о завершении автоматизированной «Экспресс-3» перевода системы на новую импортонезависимую платформу, запуске сервиса «Лист ожидания», обновлении концепции программы лояльности «РЖД Бонус» с расширением перечня услуг участникам программы, внедрении мобильной версии вебпортала РЖД, дополнении мобильного приложения «РЖД Пассажирам» сервисом оплаты билетов и услуг с помощью Mir Pay.

Ранее о совершенствовании цифровых сервисов для пассажиров рассказывал генеральный директор — председатель правления ОАО «РЖД» Олег Белозёров. В частности, он отмечал, что компания ведет разрабатывает

систему посадки пассажиров на поезд с помощью QR-кода в приложении «Госуслуги» и валидации по биометрическим персональным данным.

Источник: rzddigital.ru, 14.02.2024

Команду ИТ-интегратора Росатома в 2023 году пополнили более 1600 новых ИТ-специалистов

По итогам 2023 года АО «Гринатом» (ИТ-интегратор Госкорпорации «Росатом») привлек на работу свыше 1600 ИТ-специалистов. 28% из них составили сотрудники моложе 35 лет.

В прошлом году «Гринатом» активно привлекал молодых специалистов на стажерские программы, которые позволяют решать задачи на стыке промышленности и искусственного интеллекта. Для тех, кто только начинает свой путь в ИТ, была предложена дистанционная программа предстажировки Case Lab, которая включает в себя пять направлений. Благодаря ей участники осваивают разработку на 1С, учатся создавать и настраивать сайты в Bitrix, а также изучают основы JavaScript или Java. В 2023 году было получено 1154 заявки на прохождение стажерской программы, что на 14% больше, чем в предыдущем году. Конкуренция составила 18 человек на место (это практически в два раза выше показателя 2021 года).

Вновь пришедшие молодые специалисты и стажеры сразу занимают должности в проектных командах «Гринатома»: участвуют в создании собственного программного обеспечения, услуг и современных ИТ-решений, которыми ежедневно пользуются более 300 тысяч человек. Так, четыре стажера, пришедшие на программу в конце 2022 года, уже в начале 2023 года были приняты в штат и переведены на должности тимлидов команды разработки Единой системы интеграции корпоративных бизнес-процессов (ЕСИК БП 2.0).

Источник: rosatom.ru, 22.02.2024

«Желдорреммаш» начал подключаться к единой системе управления инженерными данными «ТМХ»

Пилотной площадкой выступает Ярославский электровозоремонтный завод (ЯЭРЗ), уже проведена интеграция с Коломенским заводом (входит в «Трансмашхолдинг», ТМХ).

Проект предполагает, что на базе программного обеспечения системы управления инженерными данными (Intermech Professional System, IPS) будет создано единое пространство группы ТМХ для работы с актуальной конструкторско-технологической документацией в электронном виде. Оно должно охватывать весь жизненный цикл локомотива — от проектирования до сервисного обслуживания.

Планируется, что в IPS будет создана общая база нормативно-справочной информации по каждой серии обслуживаемых локомотивов, что позволит автоматизировать технологическую подготовку производства, унифицировать и стандартизировать производственные процессы. Ожидаемый эффект в «Желдорреммаше» (ЖДРМ) — сокращение сроков подготовки производства и оптимизация использования ресурсов.

В ЖДРМ указывают, что сейчас идет формирование справочников по оборудованию, инструменту, оснастке и материалам по ремонту ряда серий локомотивов ТМХ — электровозов ЭП2К и 3ЭС5К, тепловозов 2ТЭ25КМ и других.

В дальнейшем планируется, что такое информационное взаимодействие в тепловозов 2TЭ25KM также установят Уссурийский Оренбургский локомотиворемонтные заводы с Брянским машиностроительным заводом. В свою очередь ремонтные заводы ЖДРМ в Улан-Удэ и Ростове-на-Дону **IPS** Новочеркасским наладят единую работу В c электровозостроительным заводом.

Ранее в этом году сообщалось, что предприятия ЖДРМ также сейчас подключаются к TOS, единой операционной системе TMX, предполагающую системное повышение производительности и качества. Сам TMX занимается активной цифровизацией производственных процессов с 2017 года, основной фокус — снижение стоимости жизненного цикла подвижного состава и повышение гибкости бизнеса.

Дополнительно производители и ремонтные компании совместно с РЖД сегодня развивают автоматизированную систему «Доверенная среда локомотивного комплекса». Она направлена на синхронизацию данных об эксплуатации и обслуживании тягового подвижного состава и перспективную реализацию предиктивного подхода к обслуживанию.

Источник: nauka.tass.ru, 24.02.2024

В России появится новый суперкомпьютер

На базе строящегося центра обработки данных (ЦОД) Сбербанка в Саратовской области появится самый мощный в стране суперкомпьютер, сообщил председатель Госдумы Вячеслав Володин.

Органы исполнительной власти региона вмести с ПАО «Сбербанк» и ПАО «Россети» договорились о строительстве крупнейшего для банка ЦОДа еще в 2020 году. Завершающий этап проекта запланирован на 2027 год. В новом ЦОД будут размещены порядка 3 тысяч стоек с вычислительным оборудованием — около 120 тысяч серверов. При этом общая площадь технологических модулей составит 62,4 тысячи квадратных метров, а пиковое потребление электроэнергии — до 82 МВт. Стоимость строительства нового дата-центра оценивается в 30 миллиардов рублей.

«Один очень важный проект, даже мегапроект, который будет реализован в Балаково, — это создание суперкомпьютера, причем самого крупного в нашей стране. Он будет реализовываться на базе ЦОД, строительство которого ведет Сбербанк. Это проект следующей очереди. Занимаюсь решением этого вопроса. Это сложно, но, надеюсь, у нас все получится», — сообщил Вячеслав Володин в своем Telegram-канале.

Строительство новых дата-центров – насущная необходимость ДЛЯ ИТ-отрасли, отечественной отметил член комитета Госдумы ПО информационной политике, информационным технологиям и связи Антон Немкин. «В условиях повсеместной цифровизации ЦОДы выступают ресурсной базой как для поддержания текущего состояния рынка, так и для его развития. Фактически дата-центры – это фундамент любой цифровизации, от надежности которого зависит ее развитие. В 2022 году мы столкнулись с дефицитом центров обработки данных ввиду введения беспрецедентных санкций. Поэтому развитие дата-центров как в части усиления их мощностей, так и в части увеличения количества самих центров - приоритетный вопрос сейчас», отметил депутат.

Пример Сбера в этом случае следует считать показательным, отметил Немкин. «Здесь стоит обратить внимание на две тенденции, которые в дальнейшем должны перениматься и другими игроками. Прежде всего, строительство центра обработки данных мирового уровня с беспрецедентными мерами защиты. Напомню, что новый ЦОД станет третьим по мощности в Европе. Второй момент — региональный аспект. Важно развивать ИТ-инфраструктуру в регионах страны. Это позволит привлечь в субъекты новые ИТ-компании», — пояснил парламентарий.

Депутат напомнил, что Президент России еще в начале года поручил увеличить мощности российских суперкомпьютеров. «Это также

принципиальная задача, особенно в вопросе развития технологий искусственного интеллекта. Суперкомпьютеры позволят сосредоточиться как на фундаментальных, так и на прикладных исследованиях в наукоемких сферах. Прежде всего, в медицине», – пояснил Немкин.

На данный момент семь российских суперкомпьютеров входят в мировой топ 500, напомнил Антон Немкин. Он также подчеркнул, что проектировка и ввод в эксплуатацию новых компьютеров уже начаты. «Ha ДНЯХ Новосибирске состоялось открытие суперкомпьютера «Сергей нового Годунов», который позволит моделировать события в самых разных сферах: от экологии до экономики. Поэтому перспективы в этом направлении у страны очень большие», – подчеркнул парламентарий.

Источник: duma.gov.ru, 27.02.2024

ГК «Солар» получила патент на технологию по оптимизации средств защиты информации на основе поведенческих паттернов

В ходе регулярных исследований по инновационным разработкам ГК «Солар» получила очередной патент на уникальную технологию оптимизации средств защиты информации для сотрудников на основе паттернов их Технология позволит оптимизировать объем необходимых поведения. аппаратных программных ресурсов ДЛЯ средств информационной безопасности, учитывающий характер коммуникаций сотрудников и рабочих процессов в компании.

Современные технические средства защиты информации, такие как программы, системы мониторинга защиты, И значительного объема аппаратных ресурсов для эффективной работы. Однако до сих пор отсутствовал подход для автоматизированной инвентаризации и оптимизации выделения ресурсов под эти инструменты. В результате это приводило к их нерациональному использованию, некорректной работе, излишнему потреблению чрезмерным затратам на обеспечение И информационной безопасности.

Новая технология значительно упростит процесс выделения аппаратных и программных ресурсов для средств информационной безопасности, что позволит повысить эффективность бизнес-процессов, оптимизировать финансовые расходы и сформировать более взвешенный подход к планированию инфраструктуры.

«Мы стремимся к созданию решения, которое оптимизирует обеспечение информационной безопасности, учитывая индивидуальные особенности

пользователей и поведенческие паттерны. Наша технология находится на стадии практической реализации, и мы уверены, что она поменяет стандарты применения средств информационной безопасности в ближайшем будущем. Получение патента на данную разработку открывает новые перспективы для развития всей российской сферы информационной безопасности, укрепляя потенциал отечественных технологий и поддерживая стратегическую цель по импортозамещению», — говорит Максим Бузинов, руководитель группы исследований Центра технологий кибербезопасности ГК «Солар».

Ключевым поставщиком данных для разработанной технологии является модуль поведенческого анализа UBA, реализованный в DLP-системе Solar Dozor, который собирает информацию о паттернах поведения пользователей. Затем технология проводит автоматическую инвентаризацию установленных средств защиты информации и выявляет группы пользователей с избыточными или недостаточными ресурсами. Таким образом, технология определяет технические ресурсы, необходимые и достаточные для различных групп пользователей на основе их специфических потребностей.

Solar Dozor – система предотвращения утечек данных и защиты от корпоративного мошенничества. Блокирует передачу конфиденциальных документов, помогает выявлять признаки корпоративного мошенничества, позволяет заниматься профилактикой инцидентов безопасности.

Источник: rt-solar.ru, 26.02.2024

«Аэроэкспресс» обновил мобильное приложение

Компания выпустила обновленную версию мобильного приложения «Аэроэкспресс» для устройств на базе операционной системы Android. Об этом CNews сообщили представители ООО «Аэроэкспресс».

В приложении представлен полностью обновленный интерфейс с минималистичным дизайном, легкими для восприятия цветовыми решениями и акцентными кнопками, которые позволяют обеспечить быстрый доступ к наиболее значимым данным и сделать поиск нужной информации более удобным.

Для удобства пользователей упрощен процесс покупки билета. Для новых пассажиров на главном экране теперь доступна схема маршрутов и конструктор тарифов, который поможет подобрать наиболее выгодный вариант по заданным параметрам поездки. Для постоянных пассажиров, которые уже точно знают, какой им нужен тариф, доступно отдельное меню покупки, которое позволит оформить билет буквально в три простых шага.

Впервые в мобильном приложении «Аэроэкспресс» появилось динамическое расписание экспресс-автобусов компании по аналогии с графиком поездов. Для его просмотра нужно выбрать в едином поле расписания нужный вид транспорта, направление и дату.

Также реализован новый блок уведомлений, где отображены плановые изменения в расписании при их наличии, и расширен функционал формы обратной связи по аналогии с сайтом компании.

«Аэроэкспресс» продолжает работу над обновлением приложения для устройств на базе операционной системы iOS.

Компания запустила собственное мобильное приложение в 2013 г., ежедневно им пользуются порядка 15 тыс. пассажиров. Мобильное приложение позволяет экономить время при покупке билетов, а также приобретать билеты по более выгодной цене: при покупке билета онлайн не позднее чем за один день до поездки стоимость стандартного билета составляет 525 руб. вместо 550. Кроме того, пользователям мобильного приложения доступно начисление баллов за совершенные поездки, которые можно использовать для дальнейшей покупки билетов со скидкой от 50% до 99% в рамках программы «Аэроэкспресс Привилегия».

Источник: cnews.ru, 27.02.20223

ЗНАЧИМЫЕ СОБЫТИЯ В ОБЛАСТИ ИТ ЗА РУБЕЖОМ

Первая схема сертификации в области кибербезопасности принята в ЕС

Страны – члены Евросоюза одобрили первую схему сертификации в области кибербезопасности по общим критериям (European Cybersecurity Scheme on Common Criteria, EUCC), сообщает в среду Агентство по сетевой и информационной безопасности Евросоюза (European Union Agency for Cybersecurity, ENISA).

Согласно закону о кибербезопасности (Cybersecurity Act), новая схема одобрена в рамках разрабатываемых сертификационных стандартов в сфере кибербезопасности EC.

Схема сертификации создаётся для того, чтобы повысить кибербезопасность процессов, услуг и товаров, имеющих отношение к информационно-коммуникационным технологиям (ИКТ) на рынке ЕС. По мнению законодателей, уровень безопасности повысится, если установить всеобъемлющий набор правил, требований к техническим стандартам и процедурам для применения в Евросоюзе.

Ожидается, что в Евросоюзе схемы сертификации, такие, как EUCC, стимулируют поставщиков ИКТ-товаров придерживаться требований в сфере сертификации в области кибербезопасности.

Источник: d-russia.ru, 31.01.2024

Цифровой форум ШОС впервые прошел в Казахстане

1 февраля 2024 года в Алматы под председательством казахстанской стороны состоялось совещание руководителей министерств и ведомств государств — членов Шанхайской организации сотрудничества, ответственных за развитие информационно-коммуникационных технологий. Участники мероприятия выразили стремление углубить взаимодействие в области развития цифровой трансформации и цифровой экономики, тем самым придав новый импульс инновационно-технологическому развитию экономик стран ШОС.

На торжественном открытии с приветственными словами выступил министр цифрового развития, инноваций и аэрокосмической промышленности РК Багдат Мусин.

«Казахстан достиг значительных успехов в сфере цифровизации, GovTech и в развитии ИТ, уверенно лидируя среди стран Центральной Азии. Устойчивый рост превратил страну в ведущую экономику в регионе, что привело к повышению уровня жизни и сокращению бедности»,— отметил Багдат Мусин.

По словам министра Казахстан зарекомендовал себя как один из мировых лидеров в области GovTech, и продукты электронного правительства высоко оценены мировыми рейтингами.

«На сегодняшний день Казахстан в рамках поддержки дружеских отношений со странами Центральной Азии предоставил GovTech-решения в Республику Таджикистан», – добавил министр.

Также министр отметил успешные казахстанские IT-стартапы – резиденты международного технопарка Astana hub. На сегодняшний день в рамках поручения главы государства по масштабированию опыта Astana Hub открыто 12 региональных технопарков.

В целях определения взаимовыгодных направлений цифрового сотрудничества и взаимодействия, а также реализации перспективных и долгосрочных совместных проектов Багдат Мусин предложил создать совместный Альянс технопарков участников стран ШОС для дальнейшего

развития инновационной экосистемы и всесторонней поддержки стартап-проектов и ИТ-компаний.

«Основная цель Альянса – это обмен стартап-проектами и опытом технопарков, оказание помощи по выходу на рынки стартапам, создание венчурного обучение совместным инкубационным фонда, акселерационным программам, обеспечение бесплатным рабочим пространством с доступом 24/7, возможность предоставления бесплатных помещений для стартапов, масштабирование решений в технопарках членов стран ШОС, а также предоставление грантов и мер поддержки», - сказал министр.

По словам министра, еще одним направлением сотрудничества для улучшения технологической связанности с глобальным миром может стать строительство волоконно-оптических линий связи. Использование высокого транзитного потенциала Казахстана обеспечит ряд существенных преимуществ по подключению к сети Интернет и позволит значительно улучшить условия для пропуска трафика на Евразийском континенте. Это позволит провести диверсификацию транзитных каналов связи и расширить участие государств в международном рынке транзита данных. Поэтому предложено рассмотреть возможность строительства ВОЛС, соединяющей страны по маршруту Россия – Казахстан – Иран, с выходом к Индийскому океану.

Также в рамках национального проекта «Доступный Интернет» в Казахстане планируется строительство крупных дата-центров для обработки и хранения транзитного трафика.

В рамках взаимодействия между странами ШОС, для увеличения транзитного потенциала, а также для создания регионального дата-хаба предлагается объединить усилие по разработке совместных баз хранения данных. В этой связи предлагается внедрить совместные проекты с участием стран ШОС, начиная с создания спутников и заканчивая реализацией цифровых платформ. Совместное создание группировок спутников на основе мощностей стран ШОС также предполагает обеспечение общего доступа к космическим всех стран-участников группы. Это повысит периодичность космической съемки одной и той же территории, что, в свою очередь, оперативного ЧС, обеспечит проведение космического мониторинга мониторинга природных ресурсов, антропогенного воздействия и т.д..

По итогам встречи стороны договорились о совместной работе по продвижению решений электронного правительства, обмене знаний об успешных практиках и изучении возможностей для совместных проектов.

В рамках развития цифровой трансформации и современных информационно-коммуникационных технологий участники совещания сошлись во мнении о необходимости дальнейшего развития сотрудничества между

государствами-членами ШОС и приемлемых для всех стран форм взаимодействия.

Следующее совещание руководителей министерств и ведомств государств-членов ШОС, ответственных за развитие ИКТ, состоится в 2025 году в Китайской Народной Республике.

Проведение цифрового форума ШОС в Казахстане инициировал Касым-Жомарт Токаев на онлайн-саммите ШОС 4 июля 2023 года. Глава государства подчеркнул, что планомерное сокращение цифрового неравенства должно стать реальным приоритетом в деятельности ШОС.

Источник: gov.kz, 02.02.2024

Мошенники использовали дипфейк изображения руководителя компании для получения от сотрудника 25 млн долларов (Гонконг)

Мошенники, которые использовали технологию дипфейк (или «глубокая подделка» — методика синтеза изображения, основанная на искусственном интеллекте), чтобы выдать себя за финансового директора международной компании во время видеозвонка, смогли обманом заставить сотрудника отправить им более 25 млн долларов США.

Финансовый работник считал, что по видеозвоноку разговаривает с финансовым директором и несколькими другими руководителями высшего звена компании. Хотя они выглядели и звучали как реальные — они были дипфейком, заявила полиция Гонконга.

Жертве было отправлено электронное письмо, в котором утверждалось, что оно от финансового директора компании. Сотрудник первоначально заподозрил, что сообщение было фишинговым, поскольку в нем содержалась просьба перевести крупную сумму денег на оффшорный счет. Однако мошенникам удалось убедить сотрудника, пригласив его принять участие в видеозвонке, на котором присутствовали предполагаемый финансовый директор и несколько других коллег, которых он узнал.

Полагая, что все участники телефонного разговора реальны, сотрудник согласился отправить более 200 млн гонконгских долларов (около 25,6 млн долларов США) на указанный счет. В ходе видеоконференции с участием нескольких человек выяснилось, что все, кого он видел, были дипфейком.

Факт мошенничества был выявлен только несколько дней спустя, когда сотрудник забеспокоился о переводе и связался с головным офисом корпорации. Ни имя работника, ни название компании не раскрываются.

По словам Кевина Вриланда, генерального менеджера компании по

аутентификации Veridas, сотрудник изначально следовал надлежащим протоколам безопасности, правильно идентифицировав атаку как потенциально связанную с фишингом. Но искусственный интеллект дал злоумышленникам преимущество.

К.Вриланд сказал, что компаниям следует внедрять обновленные и усовершенствованные методы верификации и аутентификации. Эти меры должны быть направлены на подтверждение «реальности» сотрудников. Также важно, чтобы компании информировали своих работников об опасностях дипфейков, аналогичных другим видам мошенничества. Дипфейки обычно содержат несоответствия, когда происходит движение. Например, ухо может иметь определенные неровности, или радужная оболочка глаза не отражает естественный свет.

В прошлом месяце некоммерческая организация TrueMedia объявила о создании нового инструмента, который будет использовать искусственный интеллект для борьбы с дипфейками, чтобы помешать им распространять дезинформацию на предстоящих выборах в США осенью 2024 г.

True Media заявила, что проанализирует многочасовые кадры дипфейков, чтобы обучить модель искусственного интеллекта, которая может обнаруживать поддельные видео и аудио. Для этого компания просит общественность представить примеры глубоких подделок, чтобы можно было создать более полный набор обучающих данных. True Media надеется запустить бесплатную веб-версию своего инструмента в I квартале этого года. Сначала он будет доступен журналистам, специалистам по проверке фактов.

Другие компании, включая Intel Corp. и Meta Platforms Inc., также пытаются создать инструменты, способные выявлять дипфейки.

Полиция Гонконга заявила, что недавно она столкнулась с более чем 20 случаями, связанными с использованием дипфейков для обмана систем распознавания лиц путем имитации людей на удостоверениях личности. Недавно было арестовано 6 человек в связи с мошенничеством с украденными удостоверениями личностями Гонконга. Мошенники использовали карты для создания глубоких подделок, которые могли обмануть системы распознавания лиц, а затем подали более 90 заявок на получение кредита и регистрацию банковских счетов в 2023 г.

Источник: siliconangle.com, 04.02.2024 (англ. яз.)

Техника распознавания лиц на основе камеры

Системы распознавания лиц, вычислительные инструменты, которые могут распознавать людей на изображениях или видеоматериалах, в настоящее время широко используются во всем мире. Однако некоторые пользователи и разработчики выразили обеспокоенность по поводу конфиденциальности, поскольку методы распознавания ЛИЦ ПО определению основаны изображениях, на которых запечатлены лица людей. Можно использовать методы распознавания лиц для идентификации человека по лицу без разрешения. Таким образом, в некоторых недавних исследованиях в области компьютерных наук изучалась возможность предотвращения несанкционированного распознавания лиц путем запутывания, синтеза или изменения изображений для повышения конфиденциальности пользователей.

Эту область исследований сейчас широко называют распознаванием лиц Исследователи USSLAB Университета ИЗ Чжэцзяна недавно разработали СатРго, новую технологию, предназначенную для достижения AFR на уровне датчика камеры, создавая изображения, которые могут защитить конфиденциальность лиц пользователей, не влияя на другие приложения, такие распознавание активности. Их статья, принятая NDSS 2024 предварительно опубликованная на сервере препринтов arXiv, демонстрирует предлагаемую ИМИ технику cиспользованием изображений, снятых широкодоступными камерами.

«Быстрое развитие искусственного интеллекта (ИИ) способствовало приложений компьютерного появлению различных зрения, распознают человеческую деятельность », – рассказал Tech Xplore Вэньцзюнь Чжу, соавтор статьи. «Однако конфиденциальная личная информация (PII), особенно лица на изображениях, одновременно собирается и загружается на ненадежные сторонние серверы. С этой целью мы предлагаем технологию защиты конфиденциальности лиц на основе датчиков камеры, CamPro, которая превратить обычную обеспечивающую может камеру камеру, ОНА не способна фиксировать конфиденциальность. черты лица ДЛЯ идентификации, то есть анти-распознавание лиц (AFR)».

Большинство ранее представленных подходов AFR основаны на постобработке, что, по сути, означает, что они изменяют изображения, снятые камерами, после того, как они были сняты. С другой стороны, технология CamPro, разработанная USSLAB, начинает работать только тогда, когда изображения генерируются датчиками камеры, поэтому злоумышленникам будет сложнее обойти ее. Исследователи назвали эту парадигму «сохранением конфиденциальности по рождению». «Модуль камеры обычно состоит из датчика изображения (СМОЅ или ССD) и процессора сигналов изображения

(ISP), – пояснил Чжу. «Датчик изображения преобразует воспринимаемое необработанные показания (RAW), ISP, освещение затем специализированное оборудование для обработки сигналов, преобразует RAW в стандартное изображение RGB (sRGB), соответствующее зрительным человека». Системы **ISP** являются важными современных цифровых камер и выполняют две основные функции. Во-первых, они позволяют эффективно конвертировать изображения RAW в изображения sRGB. Кроме того, они предлагают контроль над датчиками изображения, например, регулировку затвора и чувствительности ISO для реализации автоматической экспозиции (AE). «Из-за разделения конструкции датчика изображения и интернет-провайдера интернет-провайдеры часто предоставляют набор настраиваемых параметров для работы с различными датчиками», – сказал Чжу.

«СатРто использует эти настраиваемые параметры интернет-провайдера для достижения функциональности защиты конфиденциальности. Хотя первоначальная цель этих параметров — создание правдоподобного изображения, мы обнаружили, что их также можно использовать для распознавания лиц, предоставляя при этом достаточно информации для безобидных приложения визуального распознавания, например, обнаружение человека, оценка позы и т. д.». В рамках своего недавнего исследования Чжу и его коллеги в первую очередь сосредоточились на процессе гамма-коррекции камеры (т. е. гамме) и так называемой матрице цветокоррекции (ССМ).

Чтобы достичь оптимальных параметров, позволяющих распознавать людей без ущерба для их конфиденциальности, они имитировали процесс захвата изображений, а также внедрили новую технику оптимизации, основанную на состязательных сетях.

«Мы заметили, что качество защищенных изображений может не соответствовать требованиям человеческого зрения», - сказал Чжу. «Поэтому мы применяем обученный усилитель изображений для восстановления качества изображения». В отличие от других систем AFR, CamPro работает внутри ISP, камеры, настраивая существующие параметры требуя перепроектирования камеры. Это могло бы значительно упростить его развертывание в реальном мире, поскольку не повлекло бы за собой внедрение совершенно новых сенсорных устройств. «Мы считаем, что эта работа является новаторской. Она не только обеспечивает защиту конфиденциальности изображений на уровне датчиков, но также предлагает полную цепочку удаления информации до восстановления изображений и визуальных задач, и ее легко развернуть», – сказал Чжу. В первоначальных тестах было обнаружено, что СатРго хорошо обобщает различные системы идентификации ЛИЦ «черного ящика», снижая среднюю точность

идентификации лица до 0,3%. Кроме того, было обнаружено, что он устойчив к кибератакам «белого ящика», которые предполагают переобучение моделей распознавания лиц для обхода эффектов систем AFR.

«СатРго больше подходит для некоторых специализированных камер, например тех, которые используются в умных домах для обнаружения падений пожилых людей и т. д.», — сказал Чжу. «Эти камеры должны выполнять некоторые визуальные задачи, не требуя информации о лице. СатРго может эффективно предотвратить злонамеренное получение и использование информации о лице в различных сценариях».

Новая система, созданная этой командой исследователей, вскоре может быть развернута и протестирована в реальных условиях для дальнейшего изучения ее потенциала. Кроме того, CamPro может вдохновить на разработку других подходов AFR, использующих внутренние параметры камер и датчиков. «Мы обнаружили, что потенциальный злоумышленник может легко собрать конфиденциальную личную информацию из показаний датчиков», – добавил Чжу. «Мы предполагаем, что будущие приложения должны получать соответствующую информацию только из данных датчиков. Поэтому мы планируем изучить больше типов датчиков, помимо камеры, с парадигмой сохранения конфиденциальности при рождении. Что касается CamPro, мы планируем улучшить его общую производительность и попытаться сделать из нее продукт»

Источник: android-robot.com, 05.02.2024

Компания Duos получила патент на искусственный интеллект (США)

Duos Technologies Group, Inc., через свою дочернюю компанию Duos Technologies, Inc., получила патент США на использование искусственного интеллекта (AI) для обнаружения дефектов в поездах и способ его использования. Компания описывает патент, охватывающий «контролируемое машинное обучение, которое проактивно обнаруживает дефекты и идентифицирует риски схода с рельсов, устанавливая новый ориентир для повышения безопасности железнодорожной отрасли».

Использование запатентованного Duos процесса искусственного интеллекта значительно повышает эффективность механических проверок вагонов, помогая предотвращать сходы с рельсов, еще больше повышая безопасность и оптимизируя работу.

По словам технического директора Duos Джеффа Некчиа, своевременное

информации предоставление оперативной является ключевой целью технологии инспекции Duos. Этот патент охватывает технологию, которая плавно интегрирует контролируемое машинное обучение в процесс проверки и вводит функцию HITL (Human In The Loop, Человек в цикле), которая железнодорожной позволяет специалистам отрасли целенаправленные, точные и эффективные проверки. Я считаю, что патент был выдан благодаря способности Duos выполнять анализ данных изображений и метаданных с высоким разрешением в режиме реального времени, что делает его идеальным для выявления дефектов, предотвращения опасностей и обеспечения безопасности.

Как заявил генеральный директор Duos Чак Ферри, подход компании основанный на AI, меняет правила игры в отрасли. Сочетая глубокое понимание железнодорожного сектора с технологией AI, разработка Duos не только помогает предотвращать сходы поездов с рельсов, но и устанавливает новый стандарт безопасности в железнодорожной отрасли благодаря инновациям и стратегическим достижениям в области AI.

Недавно Duos заключила многолетний контракт с железной дорогой I класса, использующей технологию AI. Название железной дороги Duos не раскрыла.

Источник: railwayage.com, 07.02.2024 (англ. яз.)

Thales Group оснастит поезда лондонского метро системой консультирования машинистов

Alstom в сотрудничестве с Transport for London и оператором MTR Elizabeth Line установит на своих поездах систему консультирования машинистов GreenSpeed. Всего планируется установить систему на 70 поездов модели Aventra Class 345, которые сейчас работают на ветке Elizabeth Line лондонского метрополитена.

Система консультирования GreenSpeed разработана компанией Cubris on Transport (входит в Thales Ground Transportation Systems). Система будет рекомендовать машинистам регулировать скорость в зависимости от расписания и местоположения поезда. GreenSpeed интегрирует различные операционные системы бортовых устройств, выводя все необходимые для машиниста данные на экран планшета.

Разработка позволяет выбирать наиболее эффективный скоростной режим на маршруте, избегая относительно резких торможений и ускорений. Это поможет машинистам соблюдать расписание в наиболее

энергоэффективном режиме, сокращая расход электроэнергии/топлива и снижая износ подвижного состава.

Thales Ground Transportation Systems занимается системами сигнализации, информационной безопасности и цифровизацией железных дорог. В октябре 2023 года японская компания Hitachi Rail получила разрешение от Еврокомиссии и Управления по конкуренции и рынкам Великобритании на приобретение этого подразделения Thales Group за 1,66 млрд. евро.

Источник: techzd.ru, 08.02.2024

Автоматические телефонные обзвоны с генерируемые искусственным интеллектом голосом теперь запрещены законом (США)

Федеральная комиссия по связи США (FCC) 8 февраля объявила использование технологии клонирования голоса в автоматических телефонных звонках (робозвонках) незаконным, предоставив штатам еще один инструмент для преследования мошенников, стоящих за звонками.

Постановление вступает в силу немедленно на фоне увеличения числа таких звонков из-за технологии, которая позволяет обманывать людей, имитируя голоса знаменитостей, политических кандидатов и даже близких членов семьи.

словам председателя FCC Джессики Розенворсел, По мошенники используют сгенерированные искусственным интеллектом голоса В чтобы вымогать деньги y членов семьи, знаменитостей и дезинформировать избирателей. У генеральных прокуроров штатов теперь будут новые инструменты для борьбы с этими мошенничествами и обеспечения защиты общественности от дезинформации.

Действия FCC последовали за инцидентом в преддверии президентских праймериз в штате Нью-Гэмпшир в прошлом месяце, когда фальшивый роботизированный звонок, выдававший себя за президента Д.Байдена, призвал избирателей не голосовать на выборах. По оценкам, было сделано от 5 тыс. до 25 тыс. звонков.

Генеральный прокурор Нью-Гэмпшира Джон Формелла 6 февраля заявил, что сгенерированная искусственным интеллектом запись, сделанная так, будто это президент, была связана с двумя техасскими компаниями, в отношении которых ведется уголовное расследование.

Созданная искусственным интеллектом дезинформация, нацеленная на избирателей, побудила двух сенаторов США Эми Клобучар и Мэн Сьюзан Коллинз недавно оказать давление на Комиссию по содействию выборам США,

чтобы она предприняла шаги по борьбе с подобными кампаниями дезинформации.

Источник: cbsnews.com, 08.02.2024 (англ. яз.)

Метрополитен Лондона тестирует инструменты наблюдения с помощью AI в режиме реального времени для выявления преступлений

В лондонском метро за передвижениями, поведением и языком тела тысяч пассажиров ведет наблюдение программное обеспечение (ПО) с искусственным интеллектом (АІ), разработанное для того, чтобы определить, совершают ли они преступления или находятся в небезопасных ситуациях. ПО для машинного обучения было объединено с записями с камер видеонаблюдения в режиме реального времени, чтобы попытаться обнаружить агрессивное поведение, наличие в руках оружия или ножей, а также людей, падающих на рельсы метро или уклоняющихся от оплаты проезда.

С октября 2022 г. по конец сентября 2023 г. Департамент транспорта Лондона (TfL), который управляет городской сетью метро и автобусов, протестировал 11 алгоритмов для мониторинга людей, проходящих через станцию метро Willesden Green на северо-западе города. Это первый случай, когда транспортный орган объединил АI и видеоматериалы в реальном режиме времени для создания предупреждений, которые направлялись персоналу на станциях. Во время тестирования было обнаружено более 44 тыс. случаев, из которых 19 тыс. были переданы персоналу станций в режиме реального времени.

В соответствии с запросом по Закону о свободе информации, TfL подробно описывала как был использован широкий спектр алгоритмов компьютерного зрения для отслеживания поведения людей, пока они находились на станции. Впервые были опубликованы полные подробности судебного разбирательства по случаю выявления уклонения от оплаты проезда на большем количестве станций по всей британской столице.

В ходе судебного разбирательства в Уиллесден Грин – станции, которая до пандемии Covid-19 пропускала 25 тыс. человек в день, – система искусственного интеллекта была настроена для выявления потенциальных происшествий, чтобы позволить персоналу помогать нуждающимся людям, но она также была нацелена на борьбу с преступным и антиобщественным поведением. В предоставленных документах, подробно описывается, как модели АI использовались для обнаружения инвалидных колясок, детских

колясок, вейпинга, доступа людей в несанкционированные зоны или подвергания себя опасности, приближаясь к краю железнодорожных платформ.

Документы также показывают, как AI допускал ошибки во время испытания, например, отмечал детей, которые следовали за своими родителями через билетные барьеры, как потенциальных уклоняющихся от оплаты проезда, или не мог отличить складной велосипед от не складного.

Эксперты по защите частной жизни, ознакомившиеся с документами, ставят под сомнение точность алгоритмов обнаружения объектов. Они также говорят, что неясно, сколько людей знало об испытании, и предупреждают, что в будущем такие системы наблюдения могут быть легко расширены за счет включения более сложных систем обнаружения или программного обеспечения для распознавания лиц, которое пытается идентифицировать конкретных лиц.

По заявлению TfL, были использованы существующие изображения с ΑI видеонаблюдения, алгоритмы И «многочисленные обнаружения» для выявления моделей поведения. Предоставляя сотрудникам информацию и уведомления о передвижениях и поведении пассажиров, они, как мы надеемся, смогут быстрее реагировать на любые ситуации. В отчете также говорится, что испытание дало представление об объемах уклонении от оплаты за проезд, которое «поможет формировании правильных подходов в будущем», а собранные данные соответствуют политике компании в области обработки данных.

В настоящее время рассматривается дизайн и масштабы второго этапа испытания. Никаких других решений о расширении использования этой технологии ни на другие станции, ни на дополнительные возможности пока не принято. Любое более широкое внедрение технологии, выходящее за рамки пилотного проекта, будет зависеть от всесторонних консультаций с местными сообществами и другими соответствующими заинтересованными сторонами, включая экспертов в этой области.

Во время испытаний алгоритмы, обученные обнаруживать определенное поведение или движения, были объединены с изображениями с камер видеонаблюдения на станции метро, анализируя изображения каждую десятую долю секунды. Когда система обнаруживала 1 из 11 поведений или событий, идентифицированных как проблемные, она отправляла предупреждение на iPad или компьютер сотрудников станции. В документах говорится, что сотрудники TfL получили 19 тыс. предупреждений, по которым можно было реагировать, и еще 25 тыс. было сохранено для аналитических целей.

Система пыталась идентифицировать следующие категории: движение толпы, несанкционированный доступ, охрана, помощь в передвижении, преступность и антиобщественное поведение, человек на рельсах, раненые или нездоровые люди, такие опасности, как мусор или мокрые полы, оставленные

без присмотра предметы, застрявшие клиенты и уклонение от оплаты проезда. Каждая из них имеет несколько подкатегорий.

Дэниел Лойфер, старший аналитик группы по защите цифровых прав Access Now, говорит, что всякий раз, когда он видит какую-либо систему, осуществляющую подобный мониторинг, первое, на что он обращает внимание, — это пытается ли она выявить агрессию или преступление. «Камеры будут делать это, идентифицируя язык тела и поведение», — говорит он. «Какой набор данных вам понадобится, чтобы что-то на этом тренировать?».

В отчете TfL об испытании говорится, что он планировал включить в обучение акты агрессии, но обнаружил, что «не смог успешно их обнаружить». Отмечается, что не хватало данных для обучения AI, а другие причины не включать изображения актов агрессии в отчете были скрыты. Вместо этого система выдавала предупреждение, когда кто-то поднимал руки, что в документах описывалось как «обычное поведение, связанное с актами агрессии».

«Обучающих данных всегда недостаточно, потому что эти вещи, возможно, слишком сложны и детализированы, чтобы их можно было должным образом отразить в наборах данных с необходимыми нюансами», – продолжает Д.Лойфер, отмечая, что TfL признала о недостатке обучающих данных.

Больше всего предупреждений было выдано людям, которые потенциально могли на заплатить за поездки, перепрыгивая через закрытые турникеты или проползая под ними, толкая открытые ворота, проходя через открытые ворота или следуя за кем-то, кто заплатил. По данным TfL, уклонение от оплаты проезда обходится до 130 млн фт. ст. в год, и во время проведения тестирования было получено 26 тыс. предупреждений об уклонении от оплаты проезда.

Во время всех тестов изображения лиц людей были размыты, и данные хранились максимум 14 дней. Однако через 6 месяцев после начала испытания TfL решила не размывать изображения лиц, когда людей заподозрили в неуплате, и хранила эти данные дольше. Первоначально планировалось, чтобы персонал реагировал на предупреждения об уклонении от оплаты проезда. Однако из-за большого количества ежедневных предупреждений (в некоторые дни более 300) и высокой точности обнаружения TfL настроил систему на автоматическое подтверждение предупреждений.

Значительная часть тестирования слежения с AI была направлена на то, чтобы помочь персоналу понять, что происходит на станции, и реагировать на инциденты. Оповещения о нахождении на станции 59 людей в инвалидных колясках, что позволило персоналу станции Willesden Green, на которой нет средств доступа для инвалидных колясок, обеспечить им необходимую помощь. Между тем, было получено почти 2200 предупреждений о людях,

выходящих за пределы желтых линий безопасности, 39 — о людях, наклоняющихся за край платформы, и почти 2000 предупреждений о людях, сидящих на скамейке в течение длительного времени.

На протяжении всего тестирования наблюдался огромный рост числа публичных объявлений пассажирам отойти от желтой линии. Система также генерировала оповещения о спящих и попрошайках у входов на станцию.

TfL заявляет, что система была опробована, чтобы попытаться помочь ей улучшить качество работы персонала на своих станциях и сделать её более безопасной для пассажиров.

В отчете не содержится никакого анализа того, насколько точна система обнаружения с помощью AI; однако в разных точках её приходилось корректировать. Обнаружение объектов и выявление поведения, как правило, довольно хрупкие системы и не являются надежными, – говорит Д.Лойфер. В одном случае система выдала предупреждения о том, что люди находятся в несанкционированной зоне, в то время как на самом деле машинисты покидали поезд. Солнечный свет, попадающий на камеру, также сделал их менее эффективными, говорится в документах.

Тесты также были направлены на то, чтобы выяснить, могут ли АІ обнаружить складные или не складывающиеся велосипеды и самокаты, перевоз которых в основном запрещён на сети метро. В документах говорится, что АІ не смог провести различие между сложенным и обычным велосипедом, электронным самокатом и детским самокатом. Модель уклонения от оплаты проезда также отмечала детей. Система была настроена таким образом, чтобы не отмечать людей, чей рост был ниже турникетов.

В последние годы использование AI в общественных местах для определения поведения, передвижений или идентичности людей увеличилось — часто под видом подходов «умного города». В июле 2023 г. появились сообщения о том, что несколько станций метро Нью-Йорка используют AI для отслеживания уклонения от оплаты проезда. В Лондоне TfL заявила в декабре, что распространит свои испытания по уклонению от оплаты проезда на другие станции, хотя статус этих экспериментов неизвестен

Многие из этих систем разрабатываются в ситуациях, когда отсутствуют конкретные законы, регулирующие их использование. Нормализация мониторинга на базе AI в транспортных узлах — это неоднозначный путь к надзору, и он должен быть предметом большей прозрачности и консультаций с общественностью, говорят правозащитники.

Источник: wired.com, 08.02.2024 (англ. яз.)

Google присоединяется к C2PA, чтобы повысить прозрачность контента, созданного с помощью искусственного интеллекта (США)

Google LLC объявила, что присоединяется к Коалиции по контролю происхождения и аутентичность контента (Coalition for Content Provenance and Authenticity, C2PA) в качестве члена руководящего комитета, где она будет работать с другими участниками над способами повышения прозрачности цифрового контента.

Одной из основных целей Google является продвижение технического стандарта C2PA в отношении происхождения цифрового контента совместно с другими членами руководящего комитета, включая технологические фирмы, такие как Adobe Inc., Intel Corp., Meta Platforms Inc.¹, Microsoft Corp. и Sony Corp., а также медиа-организации, такие как BBC и Publicis Groupe.

С2РА работает над проектом под названием «Учетные данные контента», что предположительно является стандартом метаданных, защищенных от несанкционированного доступа, которые могут быть прикреплены к цифровому контенту, чтобы подтвердить историю его создания и модификации.

Объявление Google появилось в то время, когда Интернет все больше наводняется контентом, созданным искусственным интеллектом. Генеративные модели искусственного интеллекта могут использоваться практически любым человеком для создания текстов, изображений и видео, которые выглядят и ощущаются исключительно подлинными, и есть опасения, что они способствуют распространению дезинформации. Поскольку США и другие страны приближаются к выборам в конце этого года, существует острая необходимость иметь возможность идентифицировать контент, созданный искусственным интеллектом. Например, пакет искусственного интеллекта Firefly от Adobe был использован для создания 1 млрд изображений в течение 3 месяцев после запуска, в то время как ОрепАI заявила, что люди ежедневно создают более 2 млн изображений, используя ее модель DALL-E 2.

Google заявила, что изучает способы интеграции учетных данных контента C2PA в такие продукты и сервисы, как Gemini, недавно анонсированный конкурент OpenAI ChatGPT. Идея состоит в том, чтобы попытаться помочь продвигать учетные данные контента в качестве ресурса для понимания происхождения цифрового контента.

Google провела собственное исследование способов повышения прозрачности цифрового контента. К таким инициативам относятся SynthID от DeepMind, функция «Об этом изображении» в поиске Google и ярлыки YouTube для модифицированного или синтетического контента.

Глава С2РА Эндрю Дженкс сказал, что Google является ключевым

¹ Запрещенная в РФ организация

сторонником подхода организации. «Мы призываем других присоединиться к нам в расширении использования учетных данных для контента и внести свой вклад в создание более безопасной и прозрачной цифровой экосистемы», – сказал он.

Решение Google присоединиться к C2PA говорит о том, что коалиция набирает обороты. Недавно Meta Platforms внедрила стандарт C2PA в свои платформы социальных сетей, в то время как OpenAI сделала то же самое со своим генератором изображений DALL-E 3.

Одной из наиболее важных целей C2PA в настоящее время является разработка методов, гарантирующих, что его цифровые водяные знаки будут видны человеческому глазу, но это сложный процесс, требующий сбалансированного присутствия метаданных, чтобы гарантировать, что это не нарушит фактический контент.

Следует отметить, что, хотя инициатива C2PA важна, метаданные далеки от надежного решения проблемы дезинформации, генерируемой искусственным интеллектом. Это скорее помеха, чем реальная защита, поскольку их можно легко удалить с любого изображения, созданного искусственным интеллектом. OpenAI, например, в прошлом указывал, что сделать это так же просто, как сделать скриншот рассматриваемого изображения и загрузить его куда-нибудь ещё.

Источник: siliconangle.com, 08.02.2024 (англ. яз.)

Hitachi Rail испытала цифровую МПЦ на ВСМ Париж – Лион

Компания Hitachi Rail успешно завершила первые динамические испытания системы микропроцессорной централизации (МПЦ) нового поколения SEI+ на высокоскоростной линии Париж – Лион, которая является старейшей во Франции и наиболее интенсивно используемой ВСМ в Европе. Ввести МПЦ в эксплуатацию планируется в августе 2024 г. Работы выполняются в рамках контракта стоимостью 129,3 млн евро, подписанного с Hitachi Rail в декабре 2019 г.

Тестирование проводилось участке Парижском на В регионе И подтвердило корректную работу системы при пропуске испытательного поезда, оборудованного бортовым устройством европейской системы управления движением поездов ETCS. Управление МПЦ осуществлялось диспетчерского центра в Лионе, расположенного на расстоянии более 500 км от участка. В проекте задействовано более 100 чел., включая 30 сотрудников Hitachi Rail, отвечающих за разработку МПЦ SEI+.

Сложность испытаний была обусловлена возможностью их проведения только в ночное время, чтобы не прерывать коммерческие перевозки на ВСМ. Специалисты Hitachi Rail контролировали работу исполнительных постов МПЦ на линии и помогали сотрудникам Национального общества железных дорог Франции (SNCF) в диспетчерском центре в Лионе собирать и анализировать результаты испытаний.

Завершить модернизацию систем ЖАТ на BCM Париж — Лион планируется в 2025 г. За развертывание системы ETCS на этой линии отвечает компания Alstom.

Системы МПЦ нового поколения для SNCF разрабатываются в рамках проекта Argos, инициированного оператором железнодорожной инфраструктуры SNCF Réseau

Источник: zdmira.com, 08.02.2024

ОАЭ готовы стать мировым полигоном для испытаний искусственного интеллекта

Возможности генеративного искусственного интеллекта уже породили несколько юридических и этических проблем, поэтому высказанная недавно основателем OpenAI Сэмом Альтманом (Sam Altman) идея создания в ОАЭ тестового полигона для формирования правил использования новых разработок в этой сфере нашла отклик и поддержку у местных властей.

Напомним, что Сэм Альтман выступал перед аудиторией этой страны по видеосвязи, находясь в США, он заявил о необходимости создания своего рода «песочницы» в ОАЭ, опыт которой в применении новых технологий искусственного интеллекта можно было бы использовать для формулирования правил при распространении их в других странах. Сэму Альтману в последние месяцы приписывают попытки привлечь средства арабских инвесторов к нескольким своим инициативам в сфере развития бизнеса OpenAI.

Министр искусственного интеллекта, цифровой экономики и приложений для удалённой работы ОАЭ, Омар аль Олама (Omar Al Olama) в интервью Bloomberg подчеркнул, что данное государство является серьёзным игроком в сфере искусственного интеллекта, поскольку комментарии Альтмана это доказывают. По поводу использования ОАЭ в качестве полигона для разработки регуляторных ограничений в применении ИИ министр заявил следующее: «Это та возможность, в реализации которой я заинтересован лично, и мы будем к этому стремиться».

Комментируя недавно возникшие требования США к эмиратской компании G42 сократить своё присутствие в Китае, аль Олама назвал ОАЭ «очень сильным партнёром США». По его словам, вся технологическая инфраструктура ОАЭ так или иначе связана с американскими компаниями, и в обозримом будущем это не изменится. Но такое сотрудничество с США не означает, что ОАЭ не сможет работать с китайскими компаниями. Власти этой ближневосточной страны не хотели бы отказываться от взаимодействия с одним из партнёров ради сохранения благосклонности другого.

Попутно чиновник пояснил, что с 2021 года ОАЭ удаётся привлекать на работу специалистов по искусственному интеллекту. По состоянию на сентябрь прошлого года в стране работало около 120 000 профильных специалистов, тогда как всего двумя годами ранее их количество не превышало 30000 человек.

Источник: 3dnews.ru, 16.02.2024

ОАЭ стали мировым лидером по скорости сетей 5G

Объединенные Арабские Эмираты стали мировым лидером по скорости сетей пятого поколения (5G) в 2023 году и заняли первое место в регионе Ближнего Востока по обмену интернет-траффиком.

В отчете уточняется, что ОАЭ были самым быстрым рынком 5G в мире во втором квартале 2023 года. Растущая конкуренция между двумя основными сетевыми операторами страны помогла достичь средней скорости загрузки 557,63 Мбит/с. Компания etisalat (e&) стала самым быстрым оператором сетей 5G в мире со средней скоростью загрузки 680,73 Мбит/с.

В 2023 году использование цифровых подписей выросло на 216%, при этом также использовался блокчейн с участием девяти банков, шести обменных пунктов и трех страховых компаний. По данным Совета цифровой экономики ОАЭ, уровень покрытия мобильной сетью в стране по-прежнему составляет 100%.

Совет рассмотрел развитие цифровой инфраструктуры в ОАЭ и показатели внедрения технологических решений. Омар Султан Аль Олама, государственный министр искусственного интеллекта, цифровой экономики и приложений для удаленной работы, заявил, что правительство ОАЭ применяет активный подход к развитию инновационной цифровой экономики.

«Эта экономика сочетает в себе национальные навыки и технологические решения, формируя передовую модель, которая способствует достижению

целей национальной стратегии цифровой экономики за счет умножения вклада цифровой экономики в ненефтяной ВВП», – сказал министр.

Правительство ОАЭ активизирует усилия по ускорению внедрения цифровых решений в целях укрепления глобальной конкурентоспособности страны в разных областях и формирования нового цифрового будущего.

Источник: russianemirates.com, 22.02.2024

Китай создает собственные стандарты для Web3 и хочет распространить их на весь мир

Власти страны обещают сформировать и опубликовать уже второй по счету стандарт, связанный с технологиями блокчейна. На этот раз планируется распространить его за пределы страны.

Стратегический документ для стратегических замыслов

Власти Китая хотят создать собственный устав для разработчиков в области Web3, для всех, кто в пределах Китайской Народной Республики (КНР) занимается разработками технологий NFT, DApps, смарт-контрактов, взаимосовместимости блокчейнов и т.д.

Как сообщает издание Cryptonews, планы по разработке «стратегического документа» обнародованы в письме, разосланном из министерства промышленности и информационных технологий КНР.

В письме утверждается, что правительство собирается «укрепить сферу технических исследований – и надзора за ними, поддержать исследовательские учреждения в работе над взаимосовместимостью блокчейнов, приватных вычислений и смарт-контрактов».

В качестве приоритетов названы безопасности блокчейна, контроль и регламентирование соответствующих работ, а также исследования технологий конвергенции частично децентрализованных (консорциумных) блокчейнов и усовершенствования в сфере безопасности данных.

Оговаривается, впрочем, что стратегический документ имеет целью «способствовать международному обмену опытом и сотрудничеству» и, естественно, активизировать усилия в направлении международной стандартизации Web3.

Иными словами, Китай преследует целью расширить свое международное влияние и как минимум принять участие в установлении международных правил для разработчиков Web3.

Популярная механика блокчейна

Интересно, что власти КНР собираются активно популяризировать технологии Web3, для чего будут активно использовать платформы с научнопопулярным контентом. В первую очередь, публике будут рассказывать о распределенной цифровой идентичности и управлении цифровыми активами.

Китай активно внедряет технологии Web3 в таких областях как здравоохранение, образование и туризм, а также – в энергетике, финансовой сфере, защите копирайта и, естественно, охране закона.

Недавно Китай объявил, что технологии блокчейна будут использоваться и в сфере идентификации граждан, то есть, строго говоря, все внутренние паспорта 1,4 млрд граждан КНР будут перенесены на блокчейн.

«Все указывает на то, что КНР собирается сделать блокчейн остовым хребтом всей своей цифровизации», — полагает Анастасия Мельникова, директор по информационной безопасности компании SEQ. По ее словам, если эта инициатива покажет эффективность, ее вполне могут перенять другие страны, особенно те, которые находятся в ареале влияния Китая. «И тогда у него действительно будут все возможности для распространения своих правил обращения с Web3 далеко за пределы своих государственных границ», — подытожила Анастасия Мельникова.

Обещанный «устав» – уже не первый стандарт, выработанный в Китае для сферы Web3. Ранее специально созданный для этого комитет уже выпустил регламент под названием «Эталонная архитектура технологии блокчейн и распределенного учета». Где он применяется на практике, издание Cointelegraph не уточняет.

Источник: cnews.ru, 20.02.2024