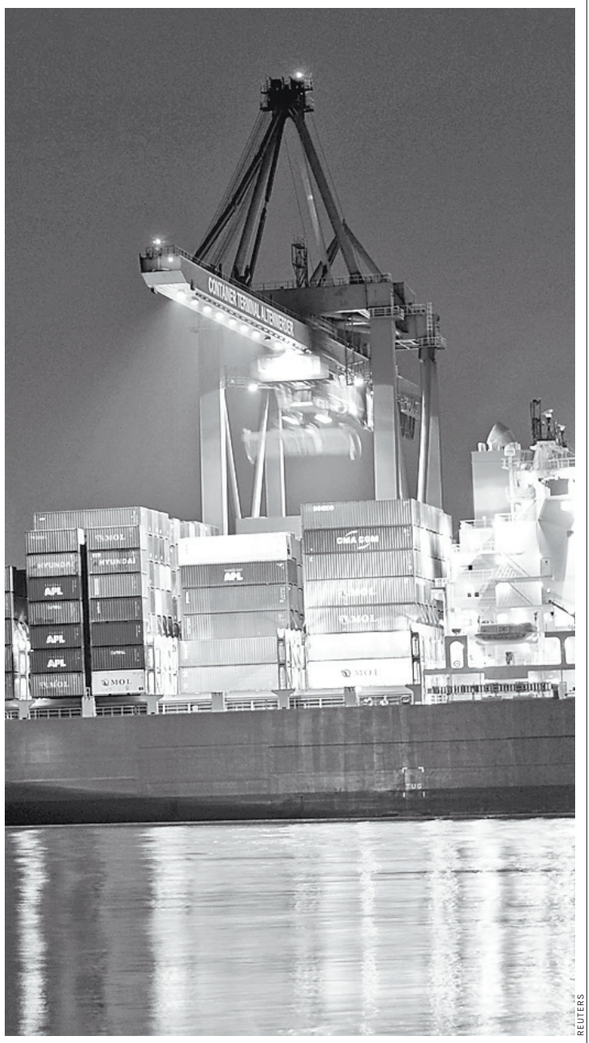
ЛОГИСТИКА



Благодаря искусственному интеллекту нелегальные автомобили не смогут через границу ни переехать, ни переплыть.

КОНТРАБАНДУ УВИДИТ КОМПЬЮТЕР

Искусственный интеллект поможет в борьбе с контрабандистами в морских портах. Ученые разработали программное обеспечение, которое может обнаружить нелегальные автомобили в контейнерах.

Морские транспортные узлы сегодня продолжают оставаться уязвимой мишенью для мошенников. Каждый месяц через них проходит огромное количество грузов, которые сложно проверить вручную. Ученые из Лондонского университета хотят научить компьютер проверять грузы вместо людей. Команда специалистов уже успешно обучила нейронную сеть определять автомобили в рентгеновских изображениях морских контейнеров. Искусственному интеллекту (ИИ) удалось идентифицировать нелегальные авто со стопроцентной точностью. Система даже заметила автомобили, которые были спрятаны за другими объектами в контейнерах.

Такие разработки помогут выявлять контрабанду и упростят работу контролеров. Цена на рентгеновскую установку и софт для программы пока не разглашается. Как и то, будет ли продаваться технология в другие страны.

Эксперты уверены, что в перспективе ИИ может кардинально изменить многие отрасли. Нейронные сети — одно из популярных сегодня направлений в разработке систем искусственного интеллекта. Они представляют собой математическую модель, максимально близко моделирующую работу человеческой нервной системы. Одно из главных преимуществ нейросетей — это способность обучаться: они могут выявлять сложные зависимости между данными и делать обобщения, с каждым разом допуская меньше ошибок.

По словам эксперта по информационным технологиям Spirit, бум развития нейронных сетей произошел в конце XX века, тогда появились нейропроцессоры, а за ним целое научное направление. Но к 2000-м интерес несколько упал. «Тогда производительность компьютеров не отвечала требованиям построения с десятками тысяч искусственных нейронов, — пояснил эксперт. — Сейчас он снова стал расти».

Помимо ИИ в портах скоро можно будет использовать и летающих дронов. «Сейчас самая большая проблема портов — логистика, — говорит профессор Сколтеха, руководитель лаборатории Интеллектуальной космической робототехники Дмитрий Тетерюков. — Дрон мог бы фактически делать каждый контейнер «прозрачным» и показывать, что внутри, то есть проецировать содержимое на поверхность контейнера с помощью специального проектора». Чтобы это стало возможным, нужна база данных, которая загружается в дрон. Тогда сотрудники портов смогут видеть всю информацию по контейнеру перед собой и даже пролистывать «странички» с характеристикой содержимого. Такие разработки уже ведутся в России в Сколтехе.

Эксперты считают, что в перспективе можно совместить использование искусственного интеллекта и дронов. На основе приложений с нейросетями можно будет создавать умные камеры с функциями видеоаналитики и распознавания лиц. Это может помочь и в поимке преступников.

ИГРЫ

ПОКЕМОН ВЫХОДИТ НА ДОРОГУ

Во всем мире набирают популярность мобильные игры, где реальность смешана с виртуальным миром. Интернет-пользователи во всех странах поголовно бросились ловить «карманных монстров», которые разбросаны по всему городу и могут притаиться в самых неожиданных местах.

Игра основана на средствах дополненной реальности, которые позволяют совмещать реальную окружающую действительность и игровое пространство. Но оказалось, что простое с виду развлечение может быть смертельно опасно.

Недавно получил огласку случай, когда игра привела к летальному исходу. В Японии мужчина, игравший в Pokemon Go, находясь за рулем автомобиля, сбил двух пешеходов. Один из них скончался на месте. Водителя арестовали, по его словам, он не увидел прохожих, так как был увлечен игрой. После инцидента разработчик игры пообещал предпринять необходимые меры по результатам расследования трагического инцидента. Но пока все связанные с игрой риски сохраняются. Использование модного приложения уже привело и к другому к ряду ДТП и различным увечьям.

Игроки так увлекаются процессом «ловли» монстров, что рискуют получить травмы или стать жертвой ограбления в реальном мире. «Особенности геолокационной игры смогли использовать реальные преступники в США: уже известны случаи, когда с помощью игры злоумышленники заманивали людей в безлюдное место и грабили их», — рассказал антивирусный эксперт «Лаборатории Касперского» Денис Макрушин. Но вряд ли такие мелочи остановят ловцов «карманных монстров».

Кроме риска физической безопасности существуют и риски информационные. Модное приложение до сих пор официально не доступно в России, но у нас уже замечены скопления «ловцов» по 100—150 человек. «Многие геймеры хотят получить доступ к игре раньше официального релиза в их регионе и скачивают приложение из сторонних источников. Эти источники могут использоваться мошенниками, которые распространяют через них вирус», — предупреждали ранее в Роскомнадзоре. Вирус позволяет перехватить контроль над устройством жертвы, похитить ее личные данные и следить за передвижениями.

Но мало того, что ваши данные оказываются под угрозой, вы еще добровольно и совершенно случайно можете сдать коммерческие тайны компании, передать изображение секретного документа, поймав, например, изображение монстра на нем. Ряд компаний, которые ввели ограничения для своих сотрудников на использование девайсов, уже внесли в список «угроз» геолокационные игры.

А бизнес из сферы торговли и обслуживания старается извлечь из новинки выгоду на крупном российском рынке. В игре к определенному месту можно приманивать «карманных монстров» и многие компании уже взяли это на вооружение. «Технология «притягивания» заложена в самой игре, можно расставлять так называемые ловушки в торговых залах, куда начнут стекаться игроки, — пояснил партнер Ingenius Systems Артур Абаджян. — К примеру, московский ЦУМ активно поддержал всеобщий ажиотаж».

По данным экспертов Hi-Tech Mail.Ru, приманки для покемонов могут увеличить проходимость заведений питания на 75 процентов. «Для владельцев ресторанов это конвертируется в реальные деньги от покупок клиентов», — пояснил руководитель Hi-Tech Mail.Ru Дмитрий Рябинин. Иными словами, связанная с реальностью игра — отличный рекламный носитель.

По словам экспертов, в следующем году ожидается запуск еще одного аналогичного проекта. «Это позволит вывести рынок мобильных развлекательных приложений на новый уровень популярности», — отметил главный аналитик Российской ассоциации электронных коммуникаций (РАЭК) Карен Казарян.

МНЕНИЕ

Денис Зеликсон,
психолог, основатель портала PosPsy:

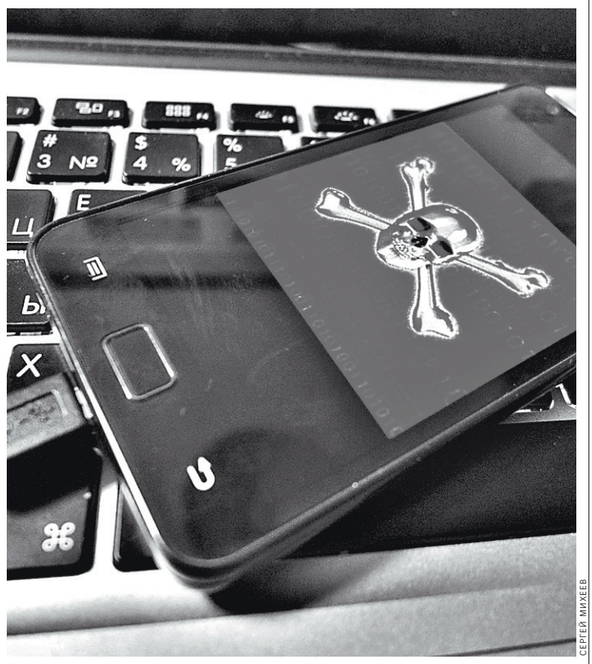
— Сенсационный интерес к игре про покемонов обусловлен особенностями восприятия информации.

Тяжело удержаться от того, чтобы не скачать приложение, если его активно используют твои друзья и о нем говорят известные личности. Информационный поток, от которого невозможно отгородиться, формирует образ игры как чего-то желанного, увлекательного и безопасного.

Обмен опытом и впечатлениями от игры с друзьями делает ее частью повседневной жизни, а человек идентифицирует себя с большим сообществом единомышленников. Польза от такого рода игр все-таки есть. Например, люди начнут больше двигаться, заставлять работать свое мышление и внимание, а также чаще общаться с другими. Так что помимо очевидного развлечения для пользователей это наконец-то мотивация выйти на улицу и совершить какую-то активность, то есть игра — это еще и своего рода фитнес-приложение. Основная опасность — развитие обсессивно-компульсивной зависимости, когда человек постоянно будет думать об игре и не отрывать голову от экрана телефона.

В погоне за виртуальными «карманными монстрами» люди не замечают, как мимо них протекает реальная жизнь.

УГРОЗЫ



Сегодня за личными данными владельцев смартфонов охотятся сотни тысяч вредоносных программ.

ТРОЯНСКИЙ КОНЬ ВСЕ ЕЩЕ ОПАСЕН

Всем хочется, чтобы компьютеры и гаджеты работали быстро и хорошо, но не все понимают, насколько большую роль в этом играют угрозы информационной безопасности и борьба с ними. За многие годы у пользователей сложилось много стереотипов и мифов про хакеров, вирусы и антивирусные компании. Эксперты по информационной безопасности раскрыли «РГ» правду о самых популярных компьютерных мифах.

Миф № 1. Самая большая опасность для компьютера — вирусы. Это не так. «Подавляющее большинство вредоносных программ (более 90 процентов) — троянцы. Они не имеют механизма саморазмножения и не являются вирусами. Но по традиции вредоносные программы в общем смысле называются вирусами, а защитные программы — антивирусами, — объяснил ведущий аналитик отдела развития «Доктор Веб» Вячеслав Медведев. — Это, кстати, привело к мнению, что для защиты от не-вирусов нужно устанавливать дополнительно к антивирусам иные средства защиты, скажем, антишпионы — против программ-шпионов. Это тоже миф».

Миф № 2. Вирусы пишут антивирусные компании, которые берут на работу хакеров. На самом деле антивирусные компании не пишут ни вирусы, ни иные вредоносные программы. Создание вредоносного ПО — уголовно наказуемое преступление. Если станет известно, что кто-то разрабатывает вирусы, этот человек рискует оказаться за решеткой. «Еще одна причина — репутационная. Число людей, задействованных в написании любого ПО, достаточно велико. А вредоносное ПО, как и обычное, продается и покупается, и не всегда сотрудники уходят по обоюдному согласию. Удержать информацию закрытой при наличии конкуренции на рынке — нереально», — объяснил Вячеслав Медведев.

Как показывают опросы, большинство киберпреступников и вирусописателей намерены работать в качестве легальных специалистов. Но компании избегают брать на работу бывших криминальных элементов. Основная причина — их ненадежность. Естественно, злоумышленник может скрыть факты о своей деятельности, но на Западе пойманные хакеры зачастую попадают в газеты, так что скрыть темное прошлое сложно.

Миф № 3. Антивирусные компании противостоят хакерам, которые пишут свои программы во имя славы. Это тоже миф. Сейчас киберпреступность — это рынок. Фактически между антивирусными компаниями и хакерами идет борьба за время. Регулярно появляются сообщения о том, что разработаны уникальные системы, позволяющие раз и на всегда победить хакеров. Например, недавно томские ученые разработали искусственный интеллект, якобы способный самостоятельно выявлять вредоносное программное обеспечение без помощи антивирусных систем. С помощью системы ученые собираются составить библиотеку индивидуального семантического следа программистов, которые пишут вредоносный код.

Охотник за вирусами должен еще и искать автора данных программ и сообщать о его деятельности в правоохранительные органы. «Стопроцентной эффективности в гонке с хакерами достичь в принципе невозможно, — заключил Медведев. — На этом фоне появляются обещания чуда — создания средств защиты, обнаруживающих 100 процентов вирусов и при этом помогающих найти авторов вредоносных программ. Но чудес не бывает».

Миф № 4. Вирусы есть только для Windows. И это не так. Вредоносные программы возможно создать практически для любой операционной системы. Некогда малоизвестная среди простых пользователей операционная система Mac OS, созданная компанией Apple, сегодня занимает второе место по популярности в мире и, увы, вызывает большой интерес у интернет-злоумышленников.

«То же происходит и с iOS: учитывая феноменальный успех iPhone и iPad, хакеры и авторы зловредов не могут себе позволить обходить эту мобильную ОС стороной, — рассказывают эксперты «Лаборатории Касперского» в своем блоге. — Что уж говорить про платформу Android: к смартфонам и планшетам на ее базе уже сегодня сотни тысяч вредоносных программ, и это число растет с каждым годом».

Миф № 5. Если на компьютере нет доступа к получению денежных средств — то ценности для хакера он не представляет. Однако аккаунты в соцсетях и на бесплатных почтовых сервисах, пароли к различным сервисам — имеют свою цену на черном рынке. Хакеры могут найти личные фотографии и шантажировать ими пользователей. А если компьютер пуст, его всегда можно сделать частью ботнета (управляемой злоумышленниками группы компьютеров) и рассылать с него спам или участвовать в атаках на ресурсы сети.

ВИДЕО

ДЛЯ ЛУНТИКА ЗАПУСТИЛИ ОТДЕЛЬНЫЙ YOUTUBE

Современные дети с раннего возраста привыкают к Интернету: играют в игры, смотрят видео. Недавнее исследование Google показало, что российские семьи проводят более 3 часов в неделю за просмотром видео на YouTube. И в такой ситуации очень важно, чтобы содержание роликов соответствовало возрасту и интересам малышей.

По данным «Лиги безопасного Интернета», большинство российских детей выходят в Сеть бесконтрольно. По результатам социологических исследований 88 процентов четырехлетних детей выходят в сеть вместе с родителями. Но уже в 8—9-летнем возрасте дети все чаще выходят в Сеть самостоятельно. К 14 годам семейное пользование сетью сохраняется лишь для 7 процентов подростков.

«У Всемирной сети есть и положительные, и отрицательные стороны. Здесь ты всегда найдешь то, что ищешь. Но какая-то информация появляется перед глазами даже вопреки желанию», — отметил сопродюсер мультсериала «Маша и Медведь» Дмитрий Ловейко. Действительно, в последнее время в Сети появляется все больше материалов агрессивного и опасного содержания, в том числе в видеороликах.

Но теперь у родителей есть возможность проконтролировать, какое видео их малыши смотрят в Интернете. Сервис YouTube запустил интерактивное приложение для всей семьи «YouTube Детям». Для приложения сервис отобрал образовательные и развлекательные ролики для малышей до восьми лет. Также в коллекцию видеозаписей вошла классика русской мультипликации и популярные новинки, которые полюбились россиянам: «Маша и Медведь», «Приключения Лунтика и его друзей», «Смешарики» и другие. По мнению экспертов в сфере детского анимационного кино, такие сервисы позволят не только обезопасить малышей от нежелательной информации в Интернете, но и помогут увеличить аудиторию отечественных мультфильмов.

Сервис также сотрудничает со многими зарубежными и российскими блогерами, которые создают развивающий контент для детей. Пользователям доступны каналы и плейлисты четырех категорий: шоу, музыка, обучение и исследование. Кроме того, можно настроить подборку видео согласно возрасту и интересам ребенка. Ведь детям разного возраста могут быть интересны разные ролики.

«Весь контент, доступный в приложении, проходит фильтр сложного алгоритма. Сервис защищен от спама и ссылок, которые ведут на не рекомендуемые детям ресурсы, — рассказала менеджер по стратегическому партнерству в сфере детского контента на YouTube в России и СНГ Светлана Барабанщикова. — Если какое-то видео все-таки покажется родителям нехорошим и сомнительным, его можно будет просто отметить флажком, и модераторы обязательно его проверят».

По словам разработчиков, дети не смогут найти в приложении мультфильмы для взрослых, типа «Южный парк» или «Симпсоны».

Приложение содержит специальные настройки для родительского контроля. Открыв их, можно сразу понять, по какому принципу приложение рекомендует контент. Родители могут сами решить, какой контент сделать доступным для ребенка. Приложение позволяет настроить доступ ко всем видео или заблокировать поиск, оставив только контент, предлагаемый на главной странице. Также можно установить таймер, чтобы ребенок не засиживался долго за просмотром мультиков, а шел делать уроки или ложился спать. Приложение само сообщит ребенку, что сессия подходит к концу.

Еще один важный момент детского YouTube: он не привязан к аккаунту Google. Так что родители могут быть уверены, что информация о том, что смотрит их ребенок, нигде не отображается и не хранится. Детский YouTube уже доступен для планшетов и смартфонов, работающих на базе Android и iOS. Кроме того, его можно смотреть с помощью SmartTV на большом экране всей семьей.

Как отмечают специалисты по информационной безопасности, чем старше дети, тем больше времени они сидят в Сети, это приводит и еще большим рискам. По данным опроса «Лаборатории Касперского», 56 процентов несовершеннолетних пользователей Интернета в России говорят, что не могут обойтись без него. И даже по этому показателю Россия обгоняет остальных участников опроса. В Европе такую сильную увлеченность демонстрируют всего лишь 30 процентов детей, в США — 38 процентов. Около 80 процентов детей в России выходят в Интернет через отдельные компьютеры в своих комнатах или через мобильные телефоны.

«Именно низкая цифровая грамотность родителей лежит в основе их беспечного отношения к интернет-активности детей. Взрослым нельзя оставлять их в одиночку в Сети, а стоит вместе осваивать новый цифровой образ жизни, — считает директор Фонда развития Интернет, доктор психологических наук, член-корреспондент РАО Галина Солдатова. — Это позволит не допускать ненужной в этом возрасте чрезмерной увлеченности Интернетом в ущерб учебе, досугу, спорту, прогулкам и живому общению».

ЭЛЬМИРА АШИРОВА

Сегодня персонажи из отечественных мультфильмов пользуются популярностью не только у детей, но и у их родителей.

ИННОВАЦИИ Чемпионов наградят медалями из смартфонов

Потянет на золото

К Олимпийским играм 2020 года медали сделают из переработанных смартфонов и другой электроники. Об этом заявили организаторы Олимпиады в Японии.

Практически вся электроника содержит множество самых разных металлов, в том числе и драгоценных — серебра и даже золота. «На печатной плате в компьютерах и смартфонах обязательно имеются золоченые детали: разъемы все золоченые, сама микросхема спаяна на золоте, контакты различных микросхем — все покрыто золотом, — рассказали эксперты НИТУ «МИСиС». — Сама основа платы — медная, золотое покрытие — напыленное или нанесенное с помощью электролиза». Но не спешите разбирать свой старый телефон или компьютер, добыча золота из электроники — непростая задача.

Аналитики Hi-Tech. Mail.ru посчитали, сколько телефонов понадобится для создания нужного количества наград к Олимпиаде. Согласно исследованию журнала CHIP, в одном телефоне в среднем содержится 0,25 грамма серебра и всего 0,024 грамма золота.

Акцент

> Для создания одной награды нужно переработать около 2000 старых телефонов

Для каждой Олимпиады создаются уникальные медали, но средний вес золотой равен 500 граммов. Однако золото в ней используется только для покрытия — всего 6 граммов, а внутри серебра на 494 грамма. Для одной награды нужно переработать около 2000 старых телефонов.

Для соревнований производят золотых медалей с запасом, но обычно не больше 170. Таким образом, процесс производства нужного количества наград потребует переработать около 340 тысяч телефонов. И это не говоря уже о серебряных и бронзовых наградах, для их создания придется собрать несколько миллионов мобильных устройств.

Процесс извлечения драгоценных металлов из устройства очень сложный и дорогостоящий. Япония одна из самых передовых стран по масштабам переработки электроники. Только за 2014 год им удалось извлечь около 143 кг золота, 1500 кг серебра и больше тысячи тонн меди из старой техники. Поэтому задача организаторов Олимпиады вполне осуществима.

По данным НИТУ «МИСиС», в России много предприятий занимаются добычей драгметаллов из вторичного сырья. Например, более 100 предприятий занимаются переработкой лома. «Если закупочная цена составляет 30—40 процентов от цены продажной, то можно дешево купить отходы изделий электронной промышленности, различные катализаторы, выделить из них детали, содержащие золото-серебро, переработать их, получить благородные металлы, а потом сдать их государству или банкам», — пояснил эксперт.

Чтобы извлечь драгметаллы из смартфона сначала нужно его разобрать, выделить алюминий, железо, а уже потом определять и перерабатывать сырье, содержащее благородные металлы. Нет технологий, способных снять только золото, нужно растворить всю основу микросхем, а потом из раствора уже извлечь золото.

ПРАВО Роботы защитят от несправедливых автоштрафов

Юристов лишат работы

Профессия судебного юриста может кануть в Лету. Ей на смену приходят боты-адвокаты, которые быстрее и дешевле оспаривают штрафы за нарушение ПДД.

Британский юридический бот за почти два года работы смог оспорить 160 тысяч штрафов за парковку в Нью-Йорке и Лондоне. Онлайн-сервис под названием DoNotPay («Не плати») отменил санкций на 4 миллиона долларов.

Сервис помогает в составлении жалоб на несправедливо выписанные штрафы за парковку, автоматически направляя их в ответственное ведомство. Самостоятельно это сделать сложно, а через юриста дорого.

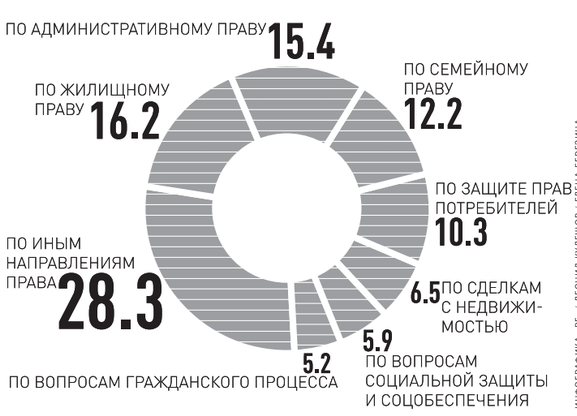
Программа бесплатна, а ее интерфейс позволяет справиться с задачей за 30 секунд. Создатель программы Джошуа Броудер изобрел ее из-за того, что сам стал жертвой несправедливости, получив за год 30 штрафов. По словам новатора, он изучил административный процесс, шаблонность которого оказалась идеальна для работы роботизированного юриста.

В скором времени поле деятельности робота расширится: можно будет онлайн получить компенсацию за задержку рейса той или иной авиакомпании по обе стороны океана. Другая возможная сфера применения бота: защита прав ВИЧ-инфицированных, беженцев, перемещенных лиц и лиц без гражданства. Кроме того, автор электронного автоюриста работает над созданием софта, который поможет сконструировать собственного робота-юриста любому, кто разбирается в той или иной отрасли юриспруденции.

В нашей стране тема юридических роботов и ботов как их проявления еще не раскрыта, сказал «РГ» основатель юридического сервиса 48Prav.ru Александр Трифонов: «Робот может быть эффективен только в понятной и логично выверенной среде. Российская правоприменительная практика не близка к идеалу. Правила часто меняются».

Говорить о том, что чат-бот стал «первым в мире роботом-юристом» не совсем правильно, отмечает генеральный директор «Конструктор документов FreshDoc.ru» Николай Пацков. Он напоминает, что в России давно действует ПО, которое позволяет составить типовые жалобы на страховые компании: например, пожаловаться в Российский союз автостраховщиков.

САМЫЕ ВОСТРЕБОВАННЫЕ ГРАЖДАНАМИ ЮРИДИЧЕСКИЕ УСЛУГИ, %
Источник: Национальная юридическая служба



ИНФОГРАФИКА «РГ» / ЛЕОНИД КУЛЕШОВ / ОЛЕНА БЕРЕЗИНА

ПОЛОСУ ПОДГОТОВИЛИ ЮЛИЯ ВОРОНИНА, ЯРОСЛАВ НИКОЛАЕВ, ТАТЬЯНА ШАДРИНА