Искусственный интеллект и современные методы отслеживания с помощью электронных устройств

Андрей Кашкаров

В последнее время расцвет цифровизации заметен практически во всех сферах приложения идей. Широкое внедрение цифрового рубля в России начнётся с июля 2025 года. С 23 февраля 2025 года требования уже частично распространются на операции по переводу цифровых рублей. Электронные устройства-помощники качественно сделали нашу жизнь как минимум совершенно иной. Вместе с нашим корреспондентом в аналитическом обзоре мы постарались разобраться в том, какую пользу и риски несёт развитие ИИ и усиление с помощью электронных устройств возможностей отслеживания перемещений и транзакций граждан, оставляющих цифровые следы.

ИИ и GPT

Нейросети с использованием функционального программирования уже настолько обучены, что пишут дипломные работы за людей. Не секрет, что можно поручить искусственному интеллекту написать статью, а самому практически ничего не делать, разве что минимально скорректировать результат. Если сегодняшний Интернет заполнен продуктами трудов копирайтеров разных уровней компетентности, то завтрашний будет состоять преимущественно из текстов нейросетей, которые учились на статьях этих копирайтеров.

Причём результаты творчества ИИ могут быть разными в зависимости от темы, задачи и электронных средств ИИ; они постоянно совершенствуются. ИИ обучается ежедневно и ежесекундно.

Результат LLM-нейросети выдают в течение нескольких секунд, при этом результаты ИИ до сих пор ещё не могут никого обмануть. Профессиональный редактор всегда распознает, написал текст человек или робот. Если же использовать ИИ как помощника, к примеру, добавить список рекомендуемой литературы по теме, чтобы результат выглядел максимально убедительным, – тогда это имеет смысл, и то с обязательной проверкой и корректировкой со стороны автора работы. Иногда полезным может быть с помощью нейросети уточнить оригинальность текста, проверить, написана ли работа «роботом» или ответственным человеком, уважающим свой труд, а главное, труд и время читателей.

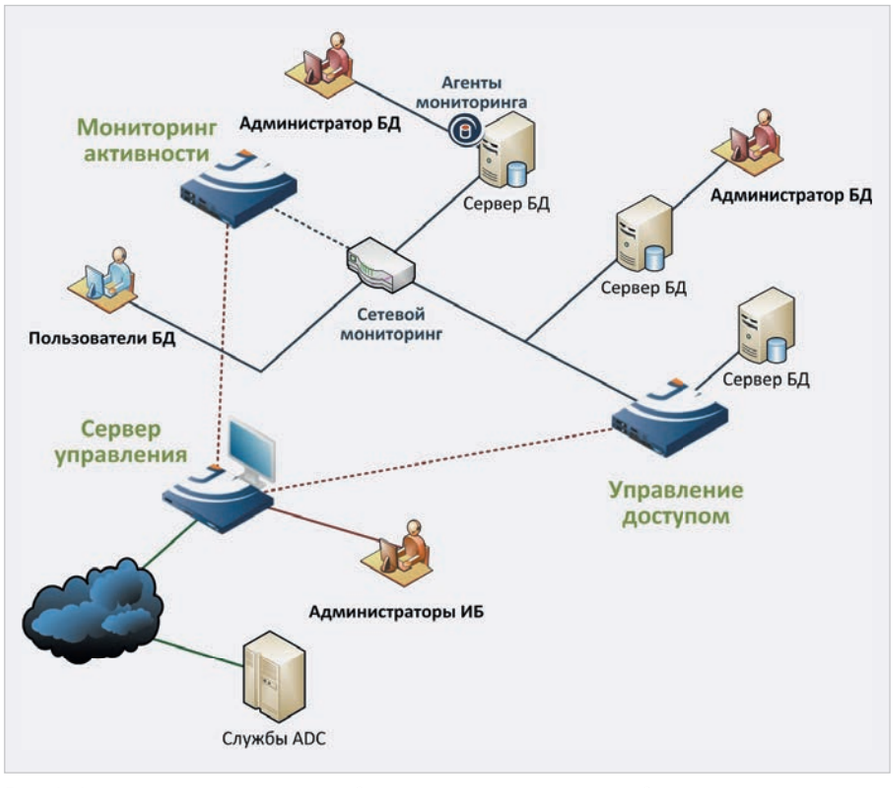

Рис. 1. Архитектура и основные функции системы защиты данных

Будущее GPT-моделей

В браузер будет встроена нейросеть, которая из входящего информационного шума сможет генерировать осмысленный контент, фильтруя условный «мусор». Всё так же будут статьи, информация и ресурсы с разной степенью ценности, актуальности и верифицируемости. Но с каждым годом будет сложнее отличить настоящие статьи-алмазы от компилированных «поддельных».

Опасность тут есть, но не для хороших СМИ и, в частности, профессиональных журналов. Ибо профессиональное сообщество по ряду критериев всегда распознает «подделку» или откровенный бред. А для нетребовательных клиентов, социальных сетей, блогеров, ориентирующихся прежде всего на презентацию и популярность, ИИ открывает кладезь возможностей. Поэтому дифференциация между качественным контентом в уважающих себя СМИ и «простыми текстовыми формами» будет нарастать. Для обывателей, незнакомых с правилами научной дискуссии и верификации информации, в том числе жалеющих время на поиски альтернативных мнений или научных исследований, информации в простом формате ответа на вопрос, сгенерированного ИИ, будет достаточно.

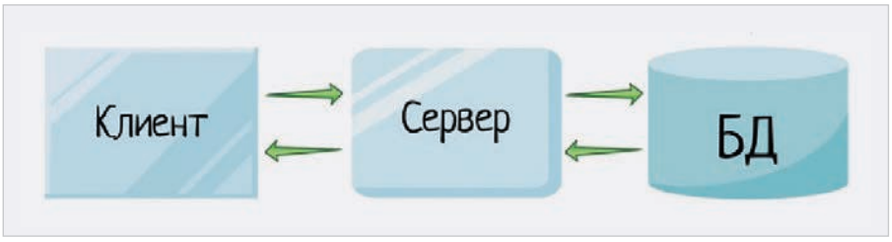

Рис. 2. Принцип работы в системе обмена данными в упрощённом виде

Рис. 3. Электронное табло в Выборге Ленинградской области

Система защиты пользовательских данных

На рис. 1 представлена архитектура и основные функции системы защиты данных.

Подсистема управления доступом представляет собой межсетевой экран, позволяющий осуществлять управление доступом к БД посредством анализа SQL-запросов пользователей. Подсистема мониторинга – модуль, обрабатывающий данные об активности пользователей, поступающих с активного сетевого оборудования, а также (при наличии такой возможности) от агентов, развёрнутых непосредственно на серверах. Агенты мониторинга – программные модули, разворачиваемые на серверах. Подсистема блокирования доступа обеспечивает перехват, анализ и соответствующее реагирование (и блокирование) SQL-запросов пользователей. Сервер управления основан на Application Defense Center (ADC), обеспечивающем доступ к актуальным обновлениям конфигурационных данных, включая сигнатуры атак и др.

В комплексе факторов это обеспечит обнаружение и оперативное реагирование на критичные для пользователей инциденты информационной безопасности, снижение вероятности финансовых и имиджевых потерь, связанных с несанкционированным доступом к данным, а также повышение эффективности взаимодействия подразделений компании, ответственных за эксплуатацию средств информатизации и обеспечение информационной безопасности за счёт реализации функций аудита баз данных вне серверов СУБД внешними средствами, которые не влияют на производительность систем [7]. Принцип работы в системе обмена данными в упрощённом виде представлен на рис. 2.

Полный видеоконтроль

В 2025 году можно с уверенностью сказать, что в России достигли уровня почти полного видеоконтроля на улицах крупных городов, а в Москве – всеобщего. Муниципалитеты и управляющие компании обычно не против установки видеокамер, потому что понимают, что те выполняют полезную функцию. Даже в малых городах с численностью жителей 30 и более тысяч человек на заре подобных проектов была идея покрывать видеонаблюдением и дворы, чтобы, как говорят, защитить жильцов от хулиганов. Однако направление пришлось свернуть, потому что выяснилось, что в провинции, где «все друг друга знают», жителям не нравится, что ведётся видеофиксация их жизни.

Особенности, польза и вред систем распознавания лиц

Системы распознавания лиц основаны на технологии Facial Recognition Technology (FRT). Это автоматическая локализация человеческого лица на изображении или видео и, при необходимости, идентификация личности человека на основе имеющихся баз данных. Интерес к этим системам очень велик в связи с широким кругом решаемых с помощью электронного оборудования задач. Например, видеонаблюдение за перекрёстками оказалось очень эффективным и стало применяться повсеместно.

На рис. 3 показано электронное табло в Выборге Ленинградской области, которое призвано информировать о движении социального транспорта. Обратите внимание, что система снабжена кнопкой вызова помощи – полиции, а также сверху осуществляется видеоконтроль. На такие, кое-где всё же работоспособные системы, затрачены по всей стране миллиарды бюджетных средств.

Видеокамеры, оснащённые ИИ, «видят», когда в помещении скапливается большое количество людей, выявляют территории, облюбованные безнадзорными, представляющими опасность для людей животными. А ведь ещё недавно бродячих собак выявляли по жалобам граждан, для чего бригадам приходилось объезжать улицы и дворы.

Устройство видеонаблюдения при обнаружении какой-либо потенциально опасной ситуации формирует сигнал для принятия службами соответствующих мер. Только наивный современный обыватель может удивляться, что все «умные» камеры подключены к мониторинговой системе центра безопасности в формате ГКУ (государственного казённого учреждения).

Аналитика несанкционированных свалок мусора, борьба с лесными (и иными) пожарами и возгораниями, контроль за такси и в целом автотранспортом, включая систему дистанционной проверки наличия полиса ОСАГО, контроль безопасности на железной дороге, примеры незаконной торговли, контроль строительных работ, чтобы «видеть» движение строительной техники и рабочих, фиксировать фактический объём строительства и следить за всеми процессами, включая соблюдение мер техники безопасности (камеры идентифицируют, в каске строитель или нет) – далеко не полный список пользы от повсеместного видеонаблюдения. Таким образом, всеохватывающее на местности видеонаблюдение решает важную задачу: ускоряет реакцию служб охраны правопорядка, уменьшает время приезда спасательных и иных специальных служб. Таково одно из аргументированных осно-

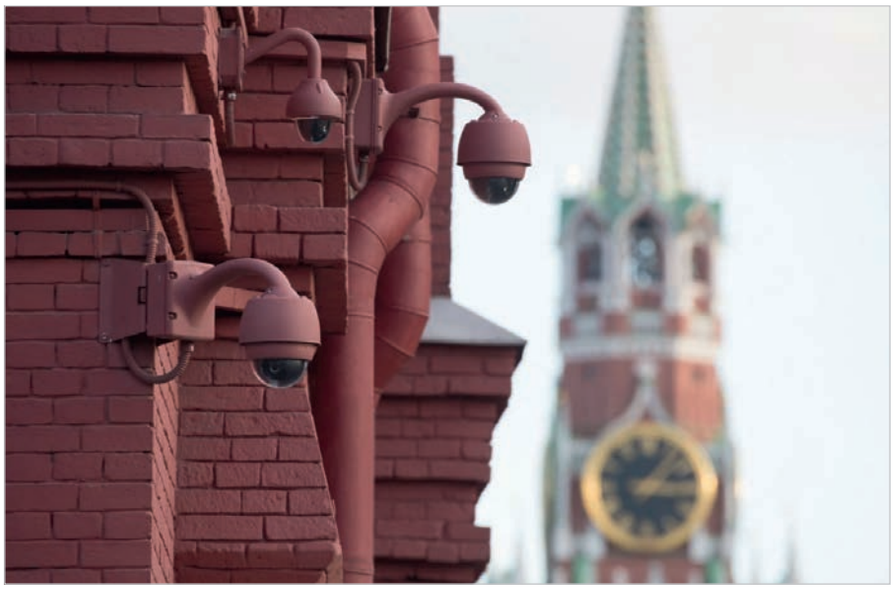

Рис. 4. Замаскированные под «ландшафт» камеры видеонаблюдения при входе на Красную площадь в Москве

Рис. 5. Видеокамеры, встроенные в терминалы и информационные табло на вокзалах и станциях

ваний для того, чтобы оборудовать подъезды и перекрёстки системой видеонаблюдения «Безопасный регион» [3]. Но есть и другая сторона медали: распознать человека, узнать, где он живёт, сейчас не очень сложно. Электронная система распознаёт человека по фотографии и находит его в базе данных, к примеру ТДИ (транспорта и дорожной инфраструктуры). После этого гражданину приходит уведомление о правонарушении или «приходят» уже за ним самим.

Кроме того, в отчётах чиновников нередко говорится, что видеокамеры системы «Безопасный регион» и устройства видеонаблюдения, установленные на социальном транспорте, научились распознавать мусор на дорогах и на остановках, «видят» ямы на дорожном покрытии и фиксируют отсутствие дорожных знаков. Однако реакции на такие «проблемы жителей» иногда приходится ждать очень долго. Поэтому видеокамера, разумеется, всё видит, но решения по ситуации всё же принимают люди. Какие решения удобны – те и принимают.

Что касается технической эволюции средств видеонаблюдения в России, то, кроме Москвы, Петербурга и ещё пары мегаполисов, где плотность установки видеонаблюдения высокая (рис. 4), в городках поменьше такая система не работает. Нет ни денег (как говорят) на её установку, ни особой нужды.

На рис. 5 показаны иллюстрации видеокамер, встроенных в терминалы и информационные табло на вокзалах и станциях. Таким образом, платформа контролируется в режиме 24/7, причём доступ к серверной системе есть не только у инспекторов-наблюдателей центров мониторинга, работающих в каждом районе и регионе, но его также может получить аттестованный сотрудник правоохранительных органов и органов госбезопасности – в любое время, из любой точки, где есть связь.

Обоснованно ожидаемое «завтра» в области электронной торговли

Уже сегодня нашла подтверждение тенденция к росту продаж розничных товаров (и не только) через маркетплейсы. Традиционная ритейл-торговля теряет доходы, материальный оборот средств и ёмкость рынка. До полного исчезновения из привычного быта магазинов разных форм ещё очень далеко, однако уже сейчас многие группы товаров люди предпочитают получать с доставкой на дом или в пунктах выдачи, заказывая их через Интернет.

В области платежей за заказы растёт число киберправонарушений. К примеру, кто-то случайно оставил в открытой сумке или на столе банковскую пластиковую карту. Потенциальный злоумышленник может скопировать её данные или же, при наличии технической возможности, создать полный её клон на основе заготовки «пластика» с чипом. При этом ответственность по закону наступает не за факт копирования, а за использование банковского инструмента в целях обогащения (платежа). Для такой работы нужно соответствующее электронное оборудование и компетенция, тем не менее число подобных случаев растёт. Понятно и то, что банковская сфера старается защищать владельцев электронных счетов (и «электронных денег») многофакторной идентификацией при транзакции не только в терминалах-банкоматах, но и в формате дистанционных интернет-платежей.

Однако одной лишь двухфакторной идентификации уже недостаточно; дополнительная идентификация будет проводиться через «Госуслуги», где предусмотрена и отдельная двухфакторная идентификация.

Ни одна современная банковская организация не проводит идентификацию по адресу электронной почты, но стремится сделать это именно через номер сотового телефона – с кодом, отправленным в формате СМС, предлагая как альтернативу (не всегда) связаться с банком через мессенджер. То есть у пользователя (обязательное условие) должен быть при себе рабочий сотовый телефон. И не только в момент авторизации, но и всегда – при совершении транзакций или дистанционных интернет-платежей. А по номеру сотового телефона легко определить владельца, IMEI-идентификатор оборудования (смартфона или кнопочного сотового телефона). То есть контроль осуществляется по месту (локация от сотового оператора), времени и действиям клиента. Иллюстрация представлена на рис. 6.

Повышение безопасности расчётов электронными средствами: плюсы и минусы

Для повышения безопасности расчётов электронными средствами планируется, в частности, обязательная регистрация через «Госуслуги» пользователей маркетплейсов, досок объявлений, сайтов по поиску работы и предложению услуг. Абоненты мобильной связи будут обязаны регистрировать передачу сим-карт третьим лицам на портале «Госуслуги», если речь не идёт о ближайших родственниках. Банки, операторов связи и интернет-магазины обяжут добавить биометрию в качестве способа авторизации в приложениях и личных кабинетах, а сотрудникам государственных организаций уже запрещено использовать иностранные мессенджеры для общения с клиентами. При этом для использования отечественными мессенджерами в рабочих целях также потребуется регистрироваться на портале «Госуслуги». Скоро для оплаты продукции банковской картой понадобятся сертификаты Минцифры России. Это ещё один дополнительный метод идентификации, актуальный в скором будущем.

Изменения федерального закона об охоте тоже не прошли без всеобщей цифровизации. Появился государственный электронный сервис документооборота «Охота», и с января 2025 года охотничий билет выдают только в электронном виде. Есть и смягчение требований к кандидатам в охотники: с сентября 2025 года охотничий билет можно иметь, начиная с 16-летнего возраста – после сдачи соответствующего экзамена.

Нас ожидает создание сервиса «государственного маркетплейса», частично интегрированного в «Госуслуги» и платформу «Почты России». Предполагается, что на нём будет возможность приобретения продукции РЭА (и не только) производителей из России – без зарубежных аналогов [6].

Однако подобные инициативы подвергают обоснованной критике. Владельцам набирающих популярность маркетплейсов избыточные требования идентификации исключительно через «Госуслуги» невыгодны. Это приведёт к значительному падению конверсии на маркетплейсах и отечественных сервисах объявлений, что может существенно усложнить развитие малого и среднего бизнеса. Кроме того, ограничения и запреты сильнее скажутся на обычных гражданах, которые, в отличие от профессиональных кибернарушителей, не умеют быстро адаптироваться к вызовам времени. Ни одним законом не установлено и не может быть установлено обязательное наличие у гражданина «кабинета» в системе «Госуслуги», равно как и наличие у человека смартфона, электронной почты и даже обычного телефона с корректно оформленной на него сим-картой.

Люди могут не иметь возможностей, технических навыков или – что важно – желания следовать государственному прессингу в этой сфере. Тем более отлично известно, что все цифровые следы, транзакции, перемещения человека так или иначе можно отследить, то есть по номеру смартфона и выходам в Интернет точно установить, где и когда человек находился в определённое время. Кстати, именно определение по сотовой связи в ходе оперативно-розыскных мероприятий правоохранительных органов помогает раскрывать большинство обычных и киберпреступлений в последние два десятка лет. Тем не менее принуждать граждан к обязательной регистрации и некорректно, и незаконно, особенно тогда, когда не отлажена система гарантированного хранения организациями разных форм собственности и сотовыми операторами персональных данных. В этом вопросе огромная проблема связана с доверием к государству граждан в разных социальных стратах.

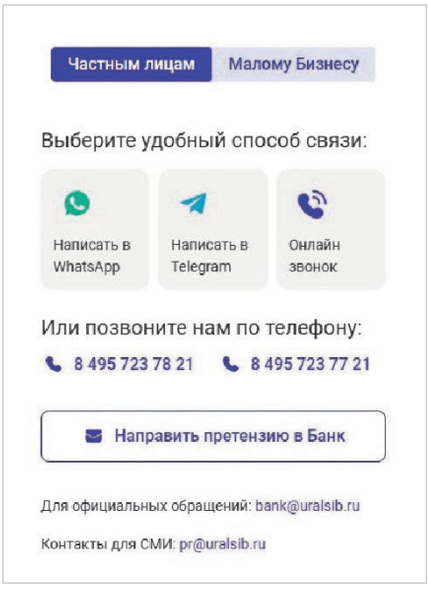

Рис. 6. Иллюстрация обязательной идентификации с помощью смартфона

Пока в этой области наблюдается огромный потенциал для совершенствования безопасных механизмов идентификации. Поэтому принудительная (избыточная) регистрация на маркетплейсах, даже если её постепенно пролоббируют конкуренты и классические торговые сети, приведёт только к оттоку покупателей.

Что касается реализации продукции отечественного производства РЭА (и не только), Минпромторг России в рамках законопроекта о «российской полке» товаров в торговых сетях предлагает, в числе прочего, обязать маркетплейсы при поиске товара рекомендовать клиентам российские аналоги иностранных брендов. Речь о маркетинговых преференциях отечественным производителям, чтобы уравнять их в конкурентных возможностях с сильными с маркетинговой точки зрения зарубежными брендами.

Перспективы QR-кода как формы для идентификации и расчётов

Сегодня развитие сетей «магазинов без персонала» – перспективное будущее розничной и мелкооптовой торговой системы – возможно при выполнении ряда условий и требований безопасности транзакций. Специалисты не спорят с возможностью единого платёжного механизма в России как альтернативы расчётов частных лиц, но важны детали.

Рис. 7. Иллюстрация-карикатура о попытках ввести QR-коды

Рис. 8. Современные способы анонимизации – маски

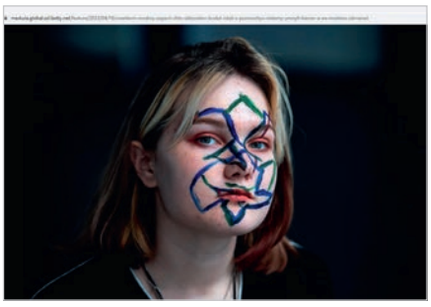

Рис. 9. Вариант противодействия идентификации по лицу с помощью краски

Рис. 10. Вариант изменения внешности фотографическим способом

Один из перспективных инструментов для транзакций – персональный QR-код. Однако в полной мере говорить о безопасности денежных расчётов с помощью QR преждевременно. Повсеместное использование возможности как платежного инструмента – тоже в далекой перспективе. А что касается экспериментов с QR-кодами – они были и ранее.

Во время всплеска эпидемии коронавируса механизм назначения и верификации QR-кода был успешно протестирован. Например, использовался в качестве пропуска в регионы, где ограничивали миграцию граждан в защитных целях, служил пропуском на массовые мероприятия, включая кинопоказы в кинотеатрах (и др.). Тогда в код, считываемый контрольными службами с помощью смартфона или сканера, подключённого к ПК с выходом в Интернет, включалась информация о персональных данных визитера, фото, информация об отсутствии заболеваний и вакцинации, срок действия кода.

Были предложены оригинальные решения, к примеру, чтобы QR-код максимально персонифицировать и сделать без ограничения срока, как номера СНИЛС и ИНН, неизменяемых на протяжении жизни, даже если гражданин меняет фамилию и имя.

Из самых оригинальных решений вспоминается печать QR-кода на одежде, на сменных шевронах с индивидуальным вышитым кодом (прикрепляемых на липучке) и т.д., вплоть до татуировок и даже возможности физического вживления чипов.

Представим, что будет, если совместить QR как идентификатор личности с банковскими инструментами. Скопировать QR можно с чужого сотового телефона, как сейчас номер и CVV (CVC) банковской карты. Таким образом, применение QR как платёжного инструмента пока не добавит безопасности, а только ослабит её.

QR-код не прикреплён к конкретному банку, но так или иначе кредитными организациями – банками применяются двойная и тройная проверки владельца счёта с помощью подтверждения СМС-сообщением или Push-уведомлением на сотовый телефон, биометрическими данными и др.

В этом смысле QR как вариант альтернативной оплаты ничем не лучше банковской карты в форме пластика – и то и другое для безопасной транзакции требуется подтверждать.

Как альтернатива, существует возможность оплаты СБП и с помощью смартфона со встроенной функцией NFC (Near Field Communication) – технологией бесконтактной передачи данных между устройствами на малых расстояниях.

До тех пор, пока QR-код не будет надёжно защищён от копирования, говорить о перспективах его как инструмента банковских транзакций и платежей в торговых точках преждевременно.

На рис. 7 шуточная иллюстрация-карикатура о попытках ввести и контролировать QR-коды на всё. Широкого охвата они не получают, но отдельные или частные эксперименты вполне возможны. Массовость магазинов без продавцов, видеоконтроля зала, бескассового узла с расчётами за приобретённый товар только по QR-коду, без поста охраны – в отдельных точках предполагает заведомые риски и потери от краж. Пока, до совершенствования системы идентификации и платежей, бескассовые магазины уместны только в охраняемых местах: бизнес- и торговых центрах. Там, где покупателя можно идентифицировать не только по QR или другому банковскому инструменту, но и по видеокартинке, по биометрическим данным.

В этом случае расчёт системы безопасности прост: идентифицировав так или иначе гражданина электронным или дистанционным способом, в случае проблем можно его найти по месту регистрации или проживания, а также в транспорте с помощью системы электронного контроля, в том числе с использованием облачных технологий, удалённых серверов, умных камер.

Способы противодействия такой идентификации тоже известны. К примеру, маски-балаклавы на лицо, проживание без регистрации, жизнь на манер дауншифтера без пользования Интернетом и сотовой связью (чтобы не оставлять цифровые следы), блокирование системы видеоконтроля разными способами и т.д. На рис. 8 показаны варианты современных масок, надеваемых на голову, применяемых для противодействия слежке умными видеокамерами. При этом такие дилетантские способы конспирации, как светоотражающая одежда, пиксельный рисунок краской на лице и иные технологии, представленные на рис. 9, 10, – уже давно не проблема для идентификации видеокамерой. О нашей ранней публикации можно прочитать в [9].

Проблематика и статистические данные по киберправонарушениям

Кибератаки на финансовый сектор бьют рекорды. От незаконных действий в цифровой сфере страдают физические и юридические лица, в том

числе госструктуры, а киберправонарушения наносят существенный вред экономике и имущественным правам людей. Суммы похищенных средств, по которым ведутся расследования, исчисляются сотнями млрд рублей в год. Пока существенное количество дел, несмотря на возрастающий профессионализм сотрудников правоохранительных органов, служб безопасности организаций, попадают в разряд «глухих», не доведённых до суда из-за сложной процедуры сбора доказательной базы. Так как в доказательной базе по уголовным делам важно обеспечить безупречно доказанную триаду: время, место, способ.

Именно из-за возрастающей активности антисоциальных элементов специальная комиссия правительства по законопроектной деятельности рекомендовала парламентариям сразу пакет законопроектов, принятие которых позволит без суда блокировать кредитной (банковской) организацией на 10–30 дней подозрительные счета; эти нормы права частично уже реализуются. По доступной статистике ясно: МВД России зарегистрировало 765,4 тыс. киберправонарушений только за 11 месяцев 2024 года. Причём 40% от этого числа составили преступления с применением информационно-телекоммуникационных технологий, общая динамика роста в этом сегменте в сравнении с тем же периодом 2023 года демонстрирует рост на 13,1%. Это максимальный показатель с 2020 года [1].

Так, ещё в 2022 году «IT-преступления» составляли 26,5% от общего числа зарегистрированных в стране правонарушений, в 2021 году – 25,8%, в 2020 – 25,0%.

В правовом поле блокировки денежных переводов обеспечены в рамках Федерального закона от 25 июля 2024 г. № 161-ФЗ «О национальной платёжной системе». Требования ЦБ о «периоде охлаждения» на банковские переводы действуют с 25 июля 2024 года.

Речь идёт о приостановке операции на два дня, если она подпадает под признаки мошенничества. Клиент банка, чей перевод был приостановлен, может подтвердить операцию не позднее следующего дня. Теперь представим себе ситуацию, что клиент банка – отправитель перевода сделал всё «по закону» и даже сохранил из банкомата бумажный чек (кое-где ещё возможно), но перевод не поступил адресату и был задержан кредитной организацией (банком). Не имея смартфона или привязки актуального номера к интернет-банку, отправитель не получит сообщения о проблеме, соответственно, не сможет в установленные сроки подтвердить транзакцию.

Системно значимые кредитные организации ежедневно «охлаждают», иными словами, блокируют около 20 тыс. денежных переводов. В этой ситуации защитные механизмы всё ещё напоминают «паровоз, нагоняющий опоздание», а не превентивные избирательные меры, причём без ущерба для законопослушных граждан, какими бы их хотелось видеть. Из-за развития самообучаемых нейросетей и чат-ботов в сфере ИИ в перспективе ближайших лет следует ожидать дальнейшего роста киберправонарушений.

Принимаемые меры

На этом фоне зафиксирована острая нехватка квалифицированных кадров в сфере информационной безопасности. В 2025 году количество вакансий специалистов по кибербезопасности увеличилось в среднем от 17 до 50% при сокращении резюме на 6%. Нижний порог дефицита обозначен в 27,3 тыс. человек.

Это реакция сегмента рынка труда на фоне роста киберугроз. Все зарекомендовавшие себя хорошие и потому ценимые руководством «безопасники» уже заняты работой, а из вузов выходят неподготовленные кадры, их необходимо дополнительно обучать практически. На фоне возросшей актуальности информационной безопасности из-за геополитической обстановки таких кадров стало не хватать. Пока рост зарплат не помогает закрывать вакансии. Эксперты ИТ-сферы полагают, что на борьбу с дефицитом кадров уйдут годы, а в течение следующих пяти лет спрос на специалистов в этой области будет постоянно увеличиваться. Повод задуматься тем молодым людям, кто серьёзно рассматривает выбор будущей карьеры в части профориентации в IT.

На рост показателей преступности с помощью ИИ влияет автоматизация бизнеса и производства и новые возможности по персонализации атак. Ежегодный прирост регистрируемых правонарушений, совершаемых с помощью ИИ, определяется примерно по числу чат-ботов и генерируемого ими контента и не фиксируется органами соцзащиты. Вместе с прогрессом искусственного интеллекта (ИИ) будут развиваться преступные методы, которые выйдут за пределы киберпространства и затронут многие аспекты жизни.

Так выглядит сегодня условная схема обогащения заинтересованных лиц за счёт социальной инженерии. Также способствует утечке персональных данных использование ИИ: как по недомыслию в компаниях, так и намеренно сотрудниками по собственной инициативе без уведомления работодателя. Это осуществляется с помощью убедительных дипфейков, автоматизации фишинга для массовых атак, а также совершенствования методов поиска уязвимостей в системах и приложениях.

Один из простых и типичных примеров, с которым уже сталкиваются сотрудники в СМИ, таков. При смене организационной формы СМИ или поглощении (расширении) организации, и в частности СМИ, персональные данные сотрудников и контрагентов должны не передаваться в другую (новую) организацию, а уничтожаться, но на практике есть массовые случаи утечек персональных данных из ликвидированных или реорганизованных фирм и учреждений. При этом доказать момент утечки данных остаётся сложной задачей.

Число киберугроз в России растёт вместе с развитием технологий. По данным «Лаборатории Касперского», в 2024 году почти 57% пользователей в России столкнулись с различными киберугрозами. В этих условиях бизнесу необходимо адаптироваться к новым вызовам и снижать риски уязвимости.

Сопутствующим шагом на федеральном уровне стало создание в России ГИС «Антикартель» ценой 240 млн рублей; таков новый механизм для предупреждения, выявления и пресечения антиконкурентных соглашений. Новая программа мониторит признаки сговора, в то время как доля картелей на торгах достигает 85–90% от всех возбуждаемых ФАС РФ антиконкурентных дел [2]. Вместе с развитием технологий генеративного ИИ и GPT повышается их доступность. Для пользователя снижается порог вхождения и стоимость владения, а значит, эти технологии будут активнее применяться для мошенничества.

Центробанк обязал банки внедрить в приложениях «спецкнопку» для жалоб на мошеннические дей-

ствия. С помощью неё пострадавшие от мошеннических действий клиенты смогут сразу же передать информацию в банк, минуя обращение в офис.

Пока это не очень простая процедура. Чтобы подать заявление, всё ещё требуется лично подать заявление: с визитом в банк или через МФЦ. Но уже с октября 2025 года банковские организации внедрят в электронные приложения «спецкнопку». Примерно такую же, как кнопка «SOS» на GPS-трекерах для детей, лиц с ограниченными возможностями здоровья, уже много лет применяемую в автомобильном транспорте. С этим «инструментом будущего» подача заявлений в банк о предполагаемом мошенничестве будет значительно упрощена.

Сегодня на дворе 2025 год, но в целом система до необходимого уровня безопасности до сих пор не доведена, несмотря на попытки заинтересованных организаций популяризовать механизмы многофакторной аутентификации владельца счёта.

Небольшой юридический ликбез и блокировка иностранных «почт»

Сервис Gmail уже отвязали от «Госуслуг». Сервис призывал пользователей сменить почту, иначе доступ к аккаунту мог быть заблокирован. Запрет на регистрацию пользователей на российских ресурсах через иностранные сервисы, такие как Google или Apple ID, вступил в силу еще в 2023 году.

Тем не менее почта Gmail в России ещё работает, а швейцарская почтовая система с двойной и тройной идентификацией под брендом Protonmail не запрещена, но условно заблокирована. Её положительная и отличительная особенность в том, что шифрование и дешифрование сообщений происходит непосредственно у отправителя и получателя электронной корреспонденции, минуя сервер. До такой степени, что даже по судебным запросам владельцы сервиса не могут технически расшифровать письма своих клиентов друг другу, так как это не предусмотрено начальной задачей и условием сотрудничества. В том числе поэтому данный сервис в России заблокирован – с его помощью нельзя отправить письма через национальные почтовые сервисы типа «Яндекс» и «Майл» (и др.) – письма просто не доходят. То же и в обратную сторону.

Парадоксально, но улучшенная защита от отслеживания, реализованная в некоторых сервисах, оказалась не только не нужна российским пользователям (их выбор не спрашивали), но её посчитали чуть ли не угрозой, потому что такие средства конфиденциальности мешают отслеживанию цифровых следов. Кому и зачем это нужно – выводы, пожалуйста, делайте сами.

А задумка швейцарских специалистов, усовершенствованная ещё в 2007–2009 годах, великолепна, поскольку «улучшенная защита от отслеживания» в Proton Mail блокирует «шпионские пиксели» (трекеры электронной почты), защищая конфиденциальность отправителей электронной почты. Функция включена по умолчанию в веб-приложении Proton Mail, приложениях для iPhone и iPad.

В веб-приложении Proton Mail пользователь получал дополнительную защиту с автоматическим удалением посторонних ссылок для отслеживания из электронных писем.

Средства контроля и легальные способы противодействия им

Существует много информации, недоступной обычному пользователю Интернета, но при желании и настойчивости можно найти и её. К примеру, особая сеть «даркнет», являющаяся скрытой частью глобальной сети. Пользователи используют специальные протоколы для осуществления связи друг с другом.

Наиболее известные технологии, позволяющие создавать и использовать закрытые информационные сети, I^2P, Tor (браузер), Freenet, есть и другие возможности. Описать все мы не можем, оставаясь в правовом поле и в связи с ограничением по объёму статьи.

Одноранговая сеть (на основе одноименного домена) I^2P обеспечивает высокую степень анонимности участников. Информация между узлами передаётся в зашифрованном виде. Предполагается, что пользователь останется неизвестен, а информация нераскрытой, даже если другие узлы будут скомпрометированы. За последние 5 лет значительно уменьшилось количество шлюзов для доступа в I^2P, поэтому использовать сеть значительно сложнее, но зато сохраняется высокая степень защиты информации и пользователей от деанонимизации. Наиболее же доступной и популярной сетью даркнета является TOR. Для того чтобы пользоваться ею, достаточно установить специальный браузер на базе Mozilla Firefox. Подробнее об этом в [8].

Не новость, что компании с разной мотивацией включали и включают средства отслеживания электронной почты в информационные бюллетени и другие маркетинговые материалы, которые отправляют пользователям по подписке или иначе. Кто-то из компаний пытался таким образом контролировать запросы потребителя для внутренней аналитики продвижения товаров (маркетинга), а кто-то изначально вкладывал в реализацию «плана» возможность отслеживания активности, местонахождения и информационных предпочтений пользователей.

Существует два распространённых типа средств отслеживания электронной почты: шпионские пиксели и отслеживающие ссылки.

Пиксель-шпион, также известный как «пиксель отслеживания» – мощный маркетинговый инструмент, включающий вставку изображения в электронное письмо в виде удалённого URL-адреса изображения. Когда пользователь открывает сообщение, содержащее пиксель-шпион, связанное изображение загружается с исходного сервера, и конфиденциальная информация отправляется обратно отправителю. Такая информация связана сведениями о факте, дате, времени открывания (прочтения) письма, содержащего трекер. Все государственные сайты в России имеют трекер-контроль. Есть ли трекинговая слежка в ваших действиях, можно уточнить самым доступным способом.

Попробуйте открыть любой сайт в Интернете, к примеру, свой аккаунт в социальной сети, дзен-рассылку или, скажем, прогноз погоды. В строке типичного браузера (а есть ещё супер-защищённые типа Tor) после открытия сайта увидите примерно такой набор символов: «https://pressfeed.ru/query/163117?utm_source=email&utm_medium=organic&utm_campaign=mailing_queries». Здесь всё, что идёт правее символа «7», начиная со знака «?», является кодовым показателем трекера. На сайтах, где трекинг не используется (их число стремительно сокращается), вы увидите чистый код, в данном приме-

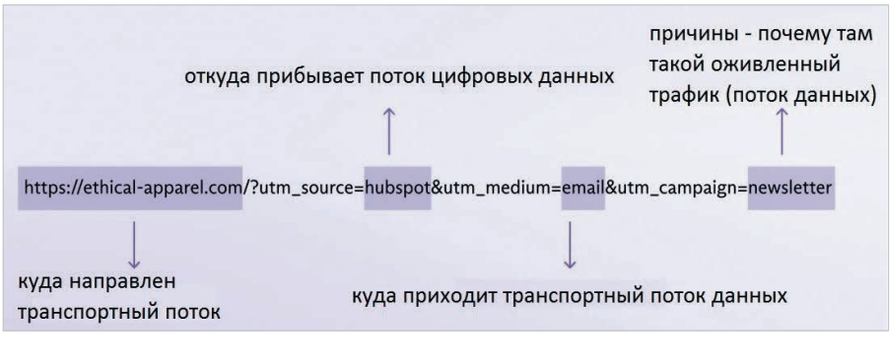

Рис. 11. Элементы кодовой строки в браузере – показатель трекеров

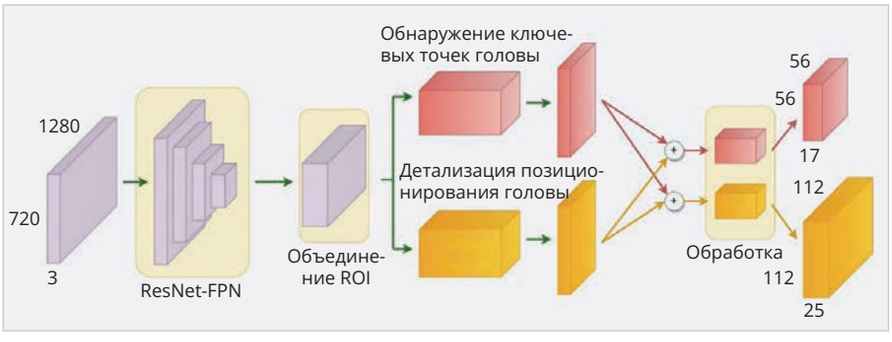

Рис. 12. Концепция определения позы человека с помощью отражённых сигналов роутера Wi-Fi через стены

ре: https://pressfeed.ru/query/163117. На рис. 11 схематично показаны элементы кодовой строки в браузере, по которым можно определить, что ваше присутствие на сайте зафиксировано с помощью трекеров.

Конкретные примеры адресной строки для статьи взяты, разумеется, произвольно. Конечно, у пользователя есть выбор, пользоваться таким контентом или нет, однако, как только вы открыли сайт, некоторые данные по месту, времени, особенностям оборудования вне зависимости от типа смартфона или ПК уже зафиксировались моментально. Таков следующий и реально действующий этап плана «контроля всего и вся» после того, как научились контролировать локацию по IMEI и сим-карте сотового телефона, в том числе местам последней их активности. Эти факторы также являются основой доказательной базы в уголовном процессе и помогают раскрывать преступления там и тогда, когда «фигурант», защищая себя, не признаётся в содеянном и для защиты прав и свобод использует положения ст. 51 Конституции России (о праве не свидетельствовать против себя и родственников).

Чтобы собрать доказательную базу, на исследование экспертам должны быть переданы электронные устройства. С санкции прокуратуры на то имеют право правоохранительные органы в процессе оперативно-розыскных мероприятий. Вот почему в первую очередь изымают на законных основаниях компьютеры, смартфоны, серверы, карты памяти и SSD.

Ни один из действующих мессенджеров пока нельзя назвать безупречным с точки зрения безопасности для пользователя. Ни один популярный мессенджер не соответствует признакам анонимного. Пока регистрация проводится по номеру телефона, переписки, по крайней мере, публичные, хранятся на серверах. Но цифровые данные сегодня контролируются не только постфактум, обращением на сервер (не все мессенджеры на серверах данные сохраняют), но есть возможность (если человек в оперативной «разработке») просмотреть всю его переписку полностью, причём в момент отправки сообщений. Перехват осуществляется на уровне информационных каналов связи, реже – провайдера.

Дополнительного шифрования открытые чаты не имеют. Да и приватные чаты тоже шифрования не имеют: идёт пересылка сообщений с устройства на устройство, минуя сервер. Это единственная и всё равно весьма условная защита.

С определёнными оговорками можно говорить о наиболее защищённых каналах на примере мессенджеров Signal, Jabber, Briar, Element. Любой из них уместно установить на свой подконтрольный сервер (при его наличии), избавившись от слежки со стороны правообладателя. В таком проекте можно ещё добавить дополнительное шифрование, и тогда уровень вашей защиты очень сильно повышается. Но такой способ работы и коммуникации далеко не всем доступен, как по уровню навыков, так и по стоимости. Поэтому большинство современных обывателей в нашей стране можно назвать государственно-подконтрольными. И в этом смысле лучше не находиться в иллюзиях.

Из всех цифровых следов уместно разделить пассивный цифровой след – остаётся при всех посещениях веб-ресурсов и авторизации на сайтах. Активный цифровой след оставляет сам пользователь – человек. Примеры тому – регистрации во всевозможных блогах, форумах, соцсетях, ведение веб-сайта. Всё, что человек осознанно публикует о себе. В этом смысле старая русская поговорка «о чём бы человек ни говорил – он говорит о себе» приобрела в современных реалиях новый и даже отчасти зловещий смысл. Ибо любой пост, публичная коммуникация, цифровой след – сродни самодоносу. То есть вы абсолютно не можете контролировать, кто и как распорядится полученной от вас или добытой спорным способом информацией.

В журнале «Современная электроника» № 2, 2023, на стр. 51 сообщается о технологии слежки за людьми с помощью Wi-Fi роутера. Тут отличились исследователи из университета Карнеги-Меллон. Вообразите, что Wi-Fi роутер превратится в устройство слежения, и это вовсе не антиутопия. Исследователи из Университета Карнеги-Меллона продвигают свою разработку как хорошую идею в помощь пожилым людям и тем, кто имеет ограниченные возможности здоровья. С помощью Wi-Fi маршрутизаторов, нейросетей и глубокого обучения разработчики смогли создать изображения субъектов в комнате в полный рост. Концепция нашла практическое подтверждение в реализации устройства Wi-Fi DensePose RCNN (рис. 12).

Причём таким же образом можно не только наблюдать за человеком (людьми) скрытно и сквозь стены, без применения видеокамер, но

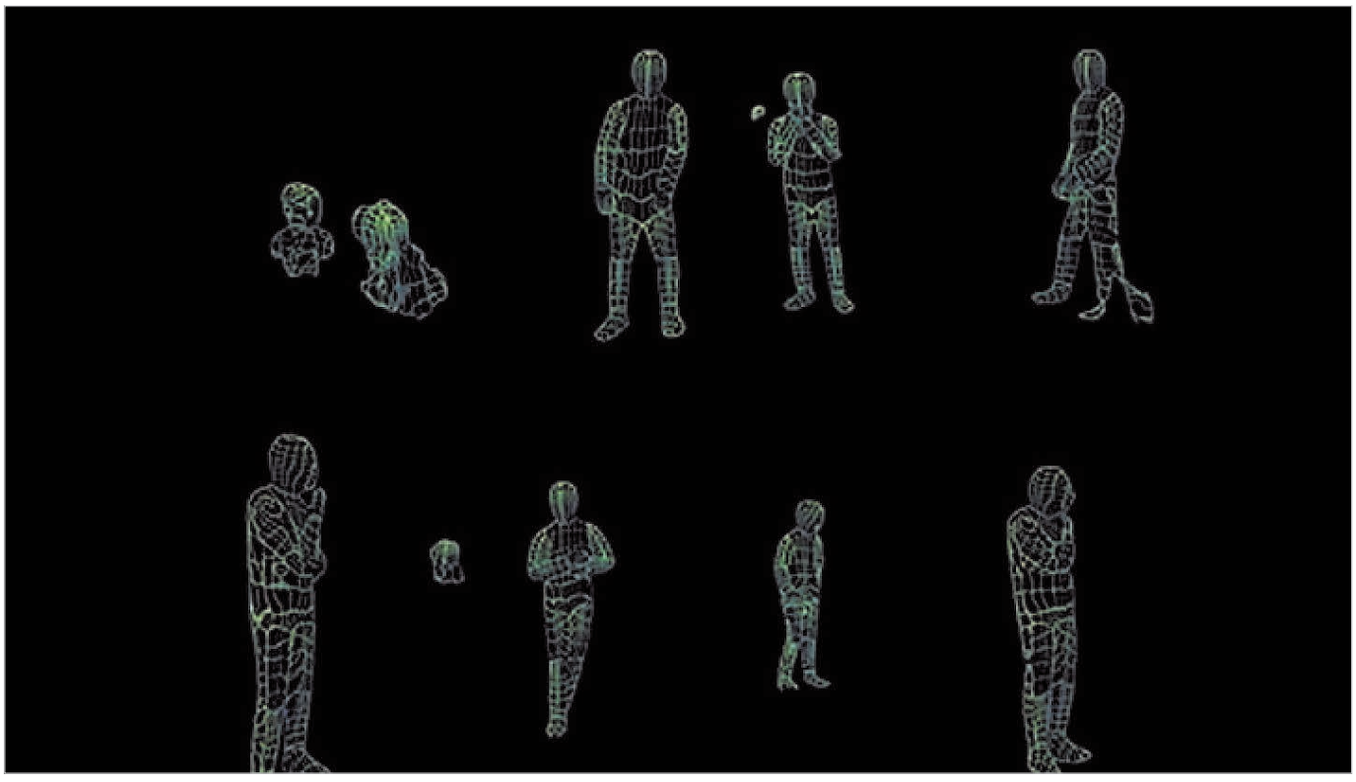

Рис. 13. Изображения, полученные с помощью ИИ и компьютерного ПО, адаптированного для системы «отслеживания» по Wi-Fi

и записывать речи и другие звуки – дистанционно. С такой разработкой нет необходимости проникать в квартиру для наблюдения за человеком, к примеру, находящимся в оперативной разработке. Достаточно «снять» в аренду квартиру по соседству. На рис. 13 представлены изображения, полученные с помощью ИИ и компьютерного ПО, адаптированного с системой «отслеживания сквозь стены» по Wi-Fi. Это вовсе не очередная конспирологическая теория, а реальность сегодняшнего дня.

Так можно получать информацию на основе изображений для прогнозирования UF-карты человеческих тел. Современные алгоритмы оценки позы двухступенчатые: сначала запускается независимый детектор человека по его физической контурной модели, чтобы сформировать рамку-ограничитель, затем проводят оценку позы, исходя из изученных баз данных изображений и поз людей.

Пока таким образом можно наблюдать за единичным объектом. Каждый элемент во входных тензорах CSI является сводным, из-за этого невозможно извлечь сигналы, соответствующие одному человеку из группы присутствующих лиц. Но это – пока. Нет сомнений в том, что обученный ИИ сможет в будущем это ограничение обойти без особых проблем.

Особенности локальных сетей

Есть ли кто-то рядом (соседи) или нет, нетрудно определить по «обзору» (видимому окружению) Wi-Fi сетей. Включив на ПК или мобильном устройстве режим доступа в Интернет по Wi-Fi, можно видеть «окружение», которое использует подключения (сети). При некотором (1–2 дня) наблюдении становится понятно, какие сети какими соседями организованы. Соответственно, определяется их присутствие.

Цифровые технологии служат существенному расширению аудитории социальных сетей, мессенджеров, даркнета и нейросетей. Транслируемая с их помощью информация несёт в себе не только ценностные смыслы, но и угрозы, при этом необходимо отметить, что деструктивные технологии наносят серьёзный урон, опережая таким образом эффективное противодействие силами безопасности.

Создаётся впечатление, что кругом одни мошенники, мешающие законопослушным людям работать, жить и размножаться. Но это не так. Большинство граждан именно законопослушные, не надо строить на этот счёт конспирологические теории.

Изменение политики (без предупреждения) в отношении клиентов – физических лиц тоже «норма вещей». Можно отслеживать телефонный трафик и собирать данные и идентификаторы, к примеру, номера IMEI близлежащих мобильных телефонов. Но дело не в претензиях, а в условной похожести стандартов обслуживания и политики работы с клиентами в большинстве известных кредитных организаций.

Бороться с дистанционным видеоконтролем и прослушкой легитимными способами практически невозможно: таково небезупречное правовое поле. Можно выключить или оставить телефон дома, если видите, что соседняя квартира насыщена антеннами, оборудованием или похожа на Байконур.

Разные варианты действий

Возникает актуальный вопрос: что делать тем, кто хочет (и имеет на то законное право) сохранить анонимность в 2025 году? Не заходить в Интернет? Понятия «анонимность» в условиях информационного общества уже не существует. Сохранить её невозможно. Чаще заинтересованные лица пытаются личность заместить. Создать личность, которая не связана с настоящей. Эта тенденция чётко выражена не только у подростков, но в целом у поколения зумеров: они портят свой цифровой след и регистри-

руются под несуществующими персональными данными, не выкладывают свои фотографии.

Выводы

Действующие и будущие защитные меры в разных (не только описанных выше) сферах направлены против кибермошенничества, в том числе для борьбы с обманом через звонки и при оформлении кредитов. Они способствуют созданию в стране правил и принципов для защиты граждан в цифровой среде.

Разумеется, обзор написан с целью информирования читателей и без намерения кому-то что-то доказать или научить противодействующим приёмам. Пока ИИ, РЭА, интегрированные в системы отслеживания соответствующего назначения, используют как помощников для человека. Этим, к сожалению, полностью исключить человеческий фактор не представляется возможным. Те или иные действия совершает конкретный человек, мы лишь сделали попытку информировать читателей о плюсах и минусах, о перспективах развития направления, совершенствования искусственного интеллекта и современных методов отслеживания с помощью электронных устройств.

Литература

1. В России в 2024 году IT-преступления достигли пика за последние пять лет (ТАСС). URL: https://tass.ru/proisshestviya/22978955.
2. В прошлом году больше 21% электронных писем для жителей Екатеринбурга оказались спамом. URL: https://www.dk.ru/news/237216838.
3. Камеры системы «Безопасный регион» стали ещё «умнее». URL: https://mskgazeta.ru/obshchestvo/kamery-sistemy-bezopasnyj-region-stali-eshe-umnee-11776.html.
4. Население мира. URL: https://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D1%81%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%97%D0%B5%D0%BC%D0%BB%D0%B8.
5. Приказ Федеральной службы безопасности Российской Федерации от 04.11.2022 № 547 «Об утверждении Перечня сведений в области военной, военно-технической деятельности Российской Федерации, которые при их получении иностранными источниками могут быть использованы против безопасности Российской Федерации». URL: https://www.garant.ru/products/ipo/prime/doc/405624539.
6. Россиян обяжут регистрироваться на Wildberries, Ozon и «Авито» через портал Госуслуг. URL: https://www.dk.ru/news/237216887.
7. Система защиты баз данных. URL: https://elvis.ru/services/application/database/.
8. Тёмные воды Интернета. URL: http://wrnews.ru/?p=7797.
9. *Кашкаров А.П.* Биоидентификация по лицу в проекции алгоритма системного анализа и обработки информации Виолы-Джонса // Современная электроника. 2023. № 4. URL: https://www.cta.ru/articles/soel/2023/2023-4/169226.
10. Wi-Fi роутер научили обнаруживать людей в комнате. URL: https://3dnews.ru/1080498/signal-wifi-moget-bit-ispolzovan-chtobi-videt-lyudey-skvoz-steni-v-detalyah.

НОВОСТИ МИРА. ЧИТАЙТЕ НА ПОРТАЛЕ WWW.CTA.RU

Отечественный ИИ помог выявить на Ямале более 500 преступников за год

Искусственный интеллект компании NtechLab – технологического партнёра Ростех – за 2025 год помог правоохранительным органам Ямало-Ненецкого автономного округа выявить более 500 преступников. В общей сложности с использованием ИИ было обнаружено свыше 1,2 тыс. человек, находившихся в розыске или числившихся пропавшими без вести.

Как работает система

Алгоритмы компьютерного зрения в режиме реального времени анализируют видеопотоки с городских камер наблюдения. За доли секунды система:

- сопоставляет изображения лиц с базами розыска;
- распознаёт биометрические признаки;
- сигнализирует правоохранительным органам при совпадениях.

Точность распознавания, по данным разработчика, превышает 99,9%.

Масштаб внедрения

На сегодняшний день нейросеть NtechLab обрабатывает видеопотоки примерно с 1,9 тыс. камер, установленных в общественных местах Ямала – на объектах транспортной инфраструктуры, улицах и городских площадях.

По данным правительства ЯНАО, каждое четвёртое преступление в регионе раскрывается с использованием ИИ-инструментов, что делает систему одним из ключевых элементов региональной программы «Безопасный город».

Планы на 2026 год: распознавание номеров

Генеральный директор NtechLab Алексей Паламарчук отметил, что компания намерена расширить сотрудничество с регионом:

«Решения NtechLab широко используются в Ямало-Ненецком автономном округе и действительно делают города безопаснее. Важно понимать, что нейросети не только помогают оперативно находить злоумышленников или потерявшихся людей, но и предотвращают преступления».

В 2026 году планируется внедрение системы распознавания автомобильных номерных знаков, которая позволит:

- быстрее выявлять угнанные автомобили;
- отслеживать подозрительный транспорт;
- усиливать контроль за транспортными потоками.

ИИ – шире, чем безопасность

В сентябре NtechLab и правительство

Ямало-Ненецкий автономный округ подписали соглашение о развитии и внедрении технологий искусственного интеллекта. Документ предусматривает использование нейросетевых решений не только в сфере безопасности, но и:

- в жилищно-коммунальном хозяйстве;
- строительстве;
- здравоохранении;
- других отраслях региональной экономики.

Итог

Опыт Ямала демонстрирует, что отечественные ИИ-решения уже вышли за рамки пилотных проектов и стали инфраструктурным инструментом управления безопасностью. Расширение функциональности – от распознавания лиц к анализу транспорта и городских процессов – указывает на формирование комплексной модели «умного региона» с опорой на российские технологии.

НОВОСТИ МИРА. ЧИТАЙТЕ НА ПОРТАЛЕ WWW.CTA.RU

В Японии установлен мировой рекорд дальней лазерной связи по воздуху

Национальный институт информационных и коммуникационных технологий Японии (NICT) объявил о мировом рекорде в области оптической связи в свободном пространстве. Учёным удалось продемонстрировать стабильную передачу данных со скоростью 2 ТБ/с по лазерному каналу на расстоянии 7,4 км в плотной городской среде Токио.

Эксперимент был проведён в апреле 2025 года, а официально объявлен 16 декабря. Это первый в мире подобный результат, достигнутый с использованием компактного ИТ-оборудования, пригодного для нестационарных сетей эпохи Beyond 5G/6G.

Рекорд в реальной городской среде

Передача данных осуществлялась по горизонтальной линии между двумя малогабаритными оптическими терминалами, установленными в городской застройке Токио – в условиях высокой атмосферной турбулентности и помех.

В эксперименте использовались два терминала:

- Full Transceiver (FX) – высокопроизводительный приёмопередатчик;
- Simple Transponder (ST) – упрощённый компактный терминал.

Несмотря на неблагоприятные атмосферные условия, система обеспечила устойчивую связь на протяжении всего эксперимента.

Общая пропускная способность канала составила 2 ТБ/с, что эквивалентно передаче примерно 10 полнометражных фильмов в формате 4K UHD за одну секунду.

Как достигли 2 ТБ/с

Рекордная скорость была обеспечена за счёт мультиплексирования по длине волны (WDM):

- 5 независимых оптических каналов;
- по 400 ГБ/с на каждый канал.

Для компенсации влияния городской атмосферы применялись:

- высокоточная система наведения луча;
- динамическая коррекция расхождения лазерного пучка;
- адаптивная оптическая коррекция в реальном времени.

Ключевое достижение – миниатюризация

Особую значимость эксперименту придаёт масштаб оборудования. Ранее терабитные скорости (1 ТБ/с и выше) демонстрировались:

- только на крупногабаритных стационарных установках;
- в лабораторных условиях;
- преимущественно в Европе.

В Азии до сих пор не удавалось превысить рубеж 100 ГБ/с в беспроводной оптической связи.

Терминалы NICT стали самыми компактными в мире (по состоянию на декабрь 2025 года) среди решений, способных обеспечить терабитную пропускную способность.

Это стало возможным благодаря комбинированному подходу:

- специально разработанные компоненты (включая телескоп с апертурой 9 см);
- модифицированные коммерческие решения;
- серийные массовые элементы.

Связь для спутников и стратосферы

Разработанные терминалы изначально ориентированы на применение за пределами наземных сетей – в том числе:

- на микро- и нано-спутниках (CubeSat);
- на стратосферных платформах HAPS;
- в гибридных воздушно-космических сетях.

Планы на ближайшие годы:

- 2026 год – демонстрация оптической связи между низкоорбитальными спутниками (~600 км) и наземными станциями со скоростью до 10 ГБ/с (в сотрудничестве с SoftBank, Kiyohara Optics и ArkEdge Space);
- 2027 год – связь между спутниками и стратосферными платформами (HAPS);
- до 2035 года – реализация мультитерабитных оптических каналов между спутниками, HAPS и наземными станциями.

Значение для Beyond 5G / 6G

Эксперимент NICT демонстрирует, что оптическая беспроводная связь способна стать:

- магистралью для будущих воздушных и космических сетей;
- альтернативой радиочастотным каналам, ограниченным спектром;
- ключевым элементом инфраструктуры Beyond 5G/6G.

Сочетание терабитных скоростей, компактности и устойчивости к атмосферным помехам делает лазерную связь реальным кандидатом на роль «оптического позвоночника» глобальных коммуникаций следующего поколения.

По прогнозам компании Micron, объём рынка памяти HBM может достичь 100 миллиардов долларов к 2028 году

Согласно Seeking Alpha, руководство Micron Technology на очередной отчётной встрече представило долгосрочный прогноз. Генеральный директор Санджей Мехротра заявил, что рынок памяти HBM будет расти на 40% в год и достигнет $100 млрд к 2028 году (против $35 млрд в текущем), опередив прежние ожидания на два года.

По его оценке, дефицит HBM и других видов памяти продлится как минимум до конца 2026 года и далее. Основным драйвером роста поставок DRAM и NAND станет переход на более передовые технологии, поскольку других способов быстро увеличить объёмы нет. Поэтому Micron увеличивает капитальные затраты на следующий год с $18 до $20 млрд, направляя их преимущественно на внедрение новых процессов, таких как «1-гамма» для DRAM, и на развитие сегмента HBM.

Рост компании подтверждается последними результатами: выручка от DRAM (включая HBM) выросла на 20% до $10,8 млрд, а от NAND – на 22% до $2,7 млрд квартал к кварталу. Общая выручка достигла $13,6 млрд, увеличившись на 21% по сравнению с предыдущим периодом и на 57% в годовом исчислении.

Несмотря на сохраняющийся дефицит, Micron уверена в своих конкурентных позициях, предлагая клиентам баланс характеристик и прибыльности. Темпы роста маржи в будущем могут замедлиться, но переход на новые технологии не окажет на неё серьёзного негативного влияния. Кроме того, компания теперь заключает долгосрочные контракты на поставку памяти на значительно более выгодных условиях, чем раньше.