International Police Association
МЕЖДУНАРОДНАЯ ПОЛИЦЕЙСКАЯ АССОЦИАЦИЯ
Российская секция

Юрий Жданов, Владимир Овчинский

ПОЛИЦИЯ БУДУЩЕГО

Москва
2018

Юрий Жданов, Владимир Овчинский
Полиция будущего. М., 2018. — 166 с.

В работе показаны возможности использования технологий новой промышленной революции в деятельности полиции. Книга представляет опыт обобщения технологических инноваций современной полиции.

Книга подготовлена в рамках проекта «Полиция будущего» Российской секции Международной полицейской ассоциации — IPA.

Оглавление

Полиция будущего — это технологии будущего

В современном мире вряд ли осталась хоть одна сфера человеческой деятельности, в которую цифровые технологии не принесли кардинальных изменений. То, что еще вчера казалось фантастикой — даже не научной, оказывается в наши дни вполне рабочим инструментом. Чтение мыслей, распознавание речи на расстоянии по движениям лица, наконец, предсказание поведения человека. Книга «Полиция будущего» предоставляет читателям обзор инноваций, от которых действительно захватывает дух.

Открываемые цифровой трансформацией возможности в полицейской деятельности в чем-то схожи с теми, которые мы видим в бизнесе. Прежде всего, это кастомизация — точечное действие, основанное на анализе огромных массивов данных. Во-вторых, создание гибких процессов, реагирующих в реальном времени на изменение ситуации. В-третьих, повышение внутренней эффективности системы, ускорение ее работы, уменьшение количества иерархических уровней. Что могут дать эти свойства в применении к полиции? Вот как формулируют ответ авторы книги: «…достижение хотя бы минимальной социальной справедливости, … развитие доступа к правосудию и защите от преступности как традиционной, так и нового типа». Они справедливо ставят вопросы прогресса полицейских технологий в глобальный контекст развития общественных отношений, возникновения «умного» общества и «умного» государства.

Наверное, все мы в свое время зачитывались детективами. При этом, следя за лихо закрученным сюжетом, мало кто отдавал себе отчет в том, что полиция — это один из фундаментальных общественных институтов, призванный ежедневно, ежеминутно находить решение чрезвычайно сложной проблемы: как совместить обеспечение общественной безопасности с вниманием к каждому человеку, его правам. Вспомним диалоги Жеглова и Шарапова из любимого многосерийного фильма 1970-х. Цифровые технологии могут предложить новые инструменты действия, но не способны решить за человека дилеммы, стоящие перед правоохранительными органами с момента их возникновения.

«Отпустить X преступников или осудить Y невиновных — что лучше?» Оттого что у нас появились системы анализа больших данных, ответ на этот вопрос нисколько не стал легче. Развитие цифровых полицейских систем уже вызывает вполне понятные опасения: некоторые их возможные применения описывают

словами «цифровой концлагерь». Смогут ли цифровые системы работать со 100%-ной точностью? Многие специалисты дают на это принципиально отрицательный ответ: если мы учим машину думать подобно человеку, мы одновременно учим ее ошибаться. Errare humanum est — с этой мыслью человечество смирилось. Но как быть с ошибающейся машиной, пусть даже процент ошибок у нее на порядок меньше человеческого? Предположим, есть полицейский-человек, приятный в общении, симпатичный и понимающий, ошибающийся в 2% случаев; и есть бездушный полицейский-робот, у которого 0,5% ошибок. К кому обратились бы лично вы?

Наверное, неслучайно новое законодательство ЕС по защите персональных данных запрещает полностью автоматические системы принятия решений на основе профилирования персональных данных, требуя во всех случаях возможности апелляции к человеку.

Очевидно, что в ближайшие годы человечеству предстоит выработать новую парадигму отношений с миром машин, сложный набор подходов, позволяющих использовать возможности цифровой трансформации и эффективно отвечать на ее вызовы. Эта работа требует глубоких знаний и широты взгляда, анализа успешных и неудачных практик из самых разных сфер жизни, с самых разных рынков.

В Московской школе управления СКОЛКОВО мы более пяти лет последовательно развиваем исследовательские и образовательные программы в области цифровой трансформации; Школа также является одной из ведущих российских площадок для дискуссий по наиболее острым вопросам новой эпохи. Я чрезвычайно рад возможности расширить свой «цифровой» кругозор благодаря книге Ю. Жданова и В. Овчинского. От всей души рекомендую ее читателям, уверен, что она не только даст им огромный объем новых знаний, но и натолкнет на важные размышления о ключевых вопросах общества и государства в цифровую эпоху.

Андрей Шаронов
Президент Московской школы управления СКОЛКОВО

Введение

Человечество осваивает новую (третью и четвертую) промышленную революцию. На наших глазах происходит взрыв технологических открытий. Но что является конечной целью этого процесса? Безусловно, построение «умного», «цифрового» общества и «умного», «цифрового» государства. И это не является простым аналогом развития «умных» городов, которые уже функционируют на планете.

«Умное», «цифровое» общество и «умное», «цифровое» государство предполагают достижение хотя бы минимальной социальной справедливости, получение всеми гражданами доступа к достижениям технологической революции и, главное, развитие доступа к правосудию и защите от преступности как традиционной, так и нового типа.

«Умное», «цифровое» общество и «умное», «цифровое» государство — это не только линейно масштабированная версия «умного» дома и «умного» города, где все наши персональные устройства и бытовые приборы подключены к Сети. Это еще и инфраструктурные и гражданские приложения, которые помогают решать общественно важные задачи и составляют **технико-политический порядок в обществе**.

Вопрос о том, какое общество и государство мы хотим, должен задаваться неразрывно с вопросами о том, какой мы хотим вид социальных связей, какой образ жизни, какие технологии, ценности и уровень безопасности.

«Умное», «цифровое» общество и «умное», «цифровое» государство — это не просто решение таких вопросов, как обеспечение прожиточного минимума и комфортной жизни. Скорее это важный аспект человеческой свободы, где корпоративные и государственные субъекты оттачивают все более изощренные средства мониторинга, контроля и манипуляции.

Корпорация RAND выпустила в 2014–2016 гг. целую серию практических исследований под общим названием «*Приоритетность криминальной юстиции*». Работы выполнялись с привлечением действующих офицеров полиции вместе с Университетом Денвера и исследовательским центром Министерства юстиции США.

RAND систематизировала следующие основные приоритеты развития:

- web-технологии как средство совместного использования информации (работа с большими объемами информации (Big Data) и учет в реальном времени сообщений сенсоров (IoT));
- общие системы электронных досье на преступников и преступления, включая единые каталоги и системы классификации;
- системы обучения офицеров полиции web-технологиям по специальным для них программам;
- разработка только тех решений, которые соответствуют общим требованиям;
- улучшение сетевой инфраструктуры с целью поддержки web-технологий, особенно для судов и исправительных учреждений;

- большая потребность в разнообразных сенсорах (сенсоры как часть интернета вещей) и соответствующих встроенных решениях, в т.ч. использование сенсоров для улучшения здоровья и безопасности офицеров;
- соблюдение гражданских прав, личной жизни и кибербезопасность.

Уже сейчас ничего нельзя спрятать, просто невозможно. Даже если информацию похоронить под землей, на основе технологий больших данных можно будет вычислить с высокой долей вероятности, что событие имело место быть. И это принципиально новый тренд, к которому мы абсолютно не готовы. И который надо будет осмыслить — в личной жизни, в политике, в бизнесе, в правоохранительной сфере.

Если говорить об «умной» полиции, то мы видим, что на некоторых полицейских участках *США и Европы* уже функционирует так называемая *система упреждающей полиции*, работа которой все меньше основывается на откликах на звонки и все больше — на патрулировании заранее известных зон с высокой степенью криминальной активности. Однако инновационность полиции этим не ограничивается, ведь криминогенные зоны можно было вычислять и раньше. На сегодня работа по поиску таких зон выполняется автоматически, что стало возможным благодаря развитию интеллектуальных систем по анализу больших данных, которые способны самостоятельно сопоставлять релевантную информацию и делать из нее выводы о повышении криминальной активности в тех или иных районах или о связях определенных людей с криминальными организациями.

Используются также новые технологии в виде *современных полицейских патрульных машин, оснащенных новейшими интегрированными ИТ-системами* взамен устаревшей радиосвязи. Такие машины способны привести полицию к месту преступления по GPS, подсказав оптимальный маршрут, а заодно показать расположение других патрульных машин в округе. Кроме того, автомобиль может проанализировать обстановку в районе патрулирования, сообщить, достаточно ли сил задействовано для предотвращения преступления, а также передать последнюю информацию о расследованиях в штаб. Меняется работа самих полицейских, которые теперь избавлены от необходимости отводить каждого подозреваемого в полицейский участок «для выяснения обстоятельств». Вместо этого сотрудник полиции фотографирует и делает видео на смартфон, подключенный к специализированным ИТ-системам, и эти фотография и видео автоматически анализируются по базе данных разыскиваемых.

«Умная» полиция активно использует **дроны**. Amazon уже оформила патент на миниатюрные дроны для патрульных полицейских. Они получили название UAVA (Unmanned Aerial Vehicle Assistant), что переводится как «беспилотный летательный аппарат-ассистент». Судя по описанию, дрон-коп будет восседать на плече патрульного, практически как попугай на плече Джона Сильвера. По

команде «взлететь» воздушный робокоп будет подниматься в воздух для выполнения команд своего «хозяина». Оснащенный видеокамерой, он сможет заглянуть туда, куда живому сотруднику заходить опасно, и тем самым избавит полицейских от неоправданного риска. А еще он сможет участвовать в преследовании преступников. Имея поддержку с воздуха, гораздо легче догнать нарушителя: находясь в поле зрения беспилотника, он имеет меньше шансов незаметно ускользнуть.

В других странах дроны борются с браконьерами и контрабандистами.

Полиция ряда американских городов в 2016 году в качестве эксперимента взяла на вооружение индивидуальные видеокамеры Body Worn. Эти похожие на смартфоны устройства включаются, записывают и выгружают видео автоматически. А в случае ранения полицейского передают сигнал тревоги диспетчеру.

Индивидуальные видеокамеры помещаются в специальный чехол под формой на уровне груди. Объектив выглядывает в отверстие-глазок. Камера включается автоматически, когда полицейский выходит из машины. Запись в режиме реального времени выгружается в защищенное облачное хранилище на Amazon Web Services.

Нагрудные камеры для полицейских Body Worn идут в комплекте с видеорегистратором для патрульных автомобилей Rocket Io T. Все эти устройства подключены к интернету вещей и действуют автономно, то есть полицейские не могут их выключить по своему желанию. И все их действия записываются как минимум с трех точек: с двух камер офицеров и из машины.

«Умная» полиция являет собой идеальное сочетание актуальной информации, личного опыта полицейских, передовых методов анализа и современного программного обеспечения, а также скоординированного и проактивного патрулирования территории подключенными патрульными машинами.

В Дубае на службу уже вышел первый робот-полицейский. Искусственный интеллект и большие данные уже перестроили работу ФБР, полиции США, Великобритании и Китая. Криминалисты все чаще обращаются за помощью к 3D-технологиям. На основе нейронных сетей разрабатываются новые полиграфы. Глобальные навигационные системы стали неотъемлемым элементом при расследовании преступлений. Огромные массивы подозреваемых в совершении уголовных преступлений и террористических актов проходят через интеллектуальные системы распознавания образов. Нейросети позволяют уже с большей долей вероятности прогнозировать преступное поведение конкретных лиц.

Эта книга открывает серию изданий Российской секции Международной полицейской ассоциации по проблемам использования новейших технологий в деятельности полиции.

Юрий Жданов,
Владимир Овчинский

Стратегический подход в использовании технологий XXI века для предотвращения преступности

Понимание и использование новых технологий в контексте преступности имеет двойственный характер. С одной стороны, данные и технологии используются преступниками для совершения криминальных действий. В этом плане новые технологии входят в число драйверов преступности. С другой стороны, *технологии являются инструментом, позволяющим успешно не только бороться с криминалом, но и профилактировать его*.

В наиболее развернутом виде данный вопрос освящен в **«Современной стратегии предупреждения преступности»** (Великобритания, март 2016). В частности, в этом документе отмечено, что эффективные протоколы обмена информацией и координации действий между центральными и региональными полицейскими структурами, бизнесом и гражданским обществом являются ключом к повышению эффективности борьбы с криминалом. *Данные и информационно-коммуникационные технологии являются важнейшим фактором создания систем эффективного обмена сведениями и результативного взаимодействия*. Если еще несколько лет назад главные усилия правоохранительных органов были направлены на создание текстовых баз данных об организованной и уличной преступности, то в настоящее время ситуация в корне изменилась.

Уже сейчас не менее 70% хранилищ данных о криминале занимают видео- и фотофайлы. С переходом городов Великобритании с населением свыше 100 тыс. человек и всех транспортных коммуникаций страны на 100%-ный охват видеонаблюдением (не позднее 2018 г.), именно видеофайлы станут основным элементом данных и материалом для профилактики преступности и проведения расследований. В настоящее время перед системой криминальной юстиции и обеспечения правопорядка в Великобритании стоит задача не только технически ответить на этот вызов, но и оснаститься средствами и инструментами, позволяющими максимально полно использовать видеоинформацию вместе с текстовой и аудиоинформацией.

Одновременно в течение последних 10 лет произошли разительные сдвиги в повседневной жизни британцев и методах ведения бизнеса. Совместно с Соединенными Штатами Великобритания стала лидером цифрового мира. Уже сегодня более 85% покупок в Великобритании совершается онлайн. Еженедельно британцы проводят в Сети не менее 15 часов. Это имеет далеко идущие последствия. С одной стороны, уже сегодня применительно к Великобритании можно говорить о единой цифровой реальности, где больше нет разделения на физическую и виртуальную. С другой стороны, Великобритания входит в мировую пятерку лидеров в робототехнике, бионауке и технологиях производства новых материалов как раз за счет эффективного использования информационно-коммуникационных технологий.

В этих условиях приходится констатировать, что *британская полиция использует большие данные и технологии, включая не только программные, но*

и физические — типа беспилотных летательных аппаратов. В отличие от ряда других стран, британский криминал уступает полицейским по своей оснащенности. Это дает определенные преимущества в ведении правоохранительной деятельности.

Чтобы наилучшим образом использовать данные и технологии, британской полиции необходимо до 2020 года не только осуществить аппаратное и программное переоснащение, но самое главное — *провести сплошное повышение квалификации полицейских, и в первую очередь на низовом уровне, изменить культуру полицейских расследований*.

Сама жизнь разрешила спор, длящийся последние 10 лет среди людей, причастных к использованию высоких технологий в британской полиции. На уровне Скотланд-Ярда, и на уровне полицейских подразделений, и в парламенте, и среди специалистов существуют две точки зрения. Одни полагают необходимым формирование мощных подразделений, специализирующихся на компьютерной преступности, на всех уровнях — от общегосударственного до регионального. Другие считают, что *в ближайшее время не останется невысокотехнологичной преступности вообще. Даже уличные преступники будут использовать те или иные плоды высоких технологий*.

Британский бизнес, особенно ключевая отрасль хозяйства — финансовая, требует от полиции качественного повышения уровня противодействия высокотехнологичной преступности. Для этого планируется *продолжить работу по формированию специализированных подразделений по киберпреступности, в том числе в рамках государственно-частных партнерств.* С другой стороны, *все британские полицейские должны иметь доступ к базам данных и современным инструментам, обеспечивающим эффективные коммуникации, профилактику и расследование преступлений с использованием информационных технологий. Наступило время, когда все британские полицейские, вне зависимости от возраста, должны пройти ускоренные курсы подготовки в области использования информационно- коммуникационных технологий*.

Поскольку значительная часть данных вообще, и медиафайлов в особенности, принадлежит в настоящее время бизнесу и муниципальным органам власти, для эффективного противодействия преступности необходимо принятие законов, обеспечивающих полиции возможность быстрого и беспрепятственного допуска к муниципальным и коммерческим базам данных без получения специальных разрешений и т.п. Это не означает вывода полиции из-под общественного контроля. Напротив, эти процедуры должны быть четко регламентированы и подконтрольны как владельцам данных, так и общественности.

Анализ больших данных

- Электронные устройства генерируют новые данные с невероятной скоростью. По информации IBM, 90% имеющихся на сегодняшний день данных

сгенерированы за два последних года. Значительная часть данных может быть использована для борьбы с преступностью или ее профилактики. Если раньше общественность интересовали прежде всего процедуры доступа к персональным и корпоративным данным, то в ближайшие годы необходимо, не дожидаясь кризиса общественного мнения, четко регламентировать доступ правоохранительных структур к *потоковым видеоданным, протоколам платежных систем и, конечно же, протоколам интернета вещей*. Уже сегодня данные (в том числе *геолокация*), получаемые со смартфонов, позволяют раскрыть многие серьезные преступления. Потенциал сведений, извлекаемых из интернета вещей, гораздо выше эффекта от данных геолокации со смартфона, хотя это и сложно представить.

- Сам по себе гигантский, постоянно возрастающий объем данных не обязательно облегчает работу полиции в части профилактики и борьбы с организованной преступностью. *Зачастую избыток сведений оказывается еще более вредным, чем недостаток*. Полицейские, не владеющие соответствующими навыками, не только не могут найти в них цифровые доказательства совершенного преступления либо признаки готовящегося, но и связывают с цифровыми доказательствами избыточные надежды. Эту проблему не решить только проведением обучения.

Современные информационные базы столь сложны, массивны и быстро пополняемы, что напрямую потребитель ими не пользуется нигде — ни в государственных учреждениях, ни в бизнесе. Сегодня одной из наиболее высокооплачиваемых и развивающихся профессий является специалист и *аналитик данных*. Это люди, которые проектируют базы и хранилища данных, а также обеспечивают пользователям возможность воспринимать данные при помощи визуальных и дружественных интерфейсов. В Великобритании подобных специалистов не хватает даже для бизнеса, поэтому британские компании и банки ищут их по всему миру. В британской полиции в настоящее время нет ни одной должностной позиции аналитика и специалиста данных. Это положение планируется в кратчайшее время исправить.

Если совместить три компонента — создание мощных, доступных вплоть до низового уровня баз и хранилищ данных; укомплектованность полиции дата-аналитиками и дата-специалистами; повышение уровня компьютерной грамотности полицейских вплоть до низового уровня,— британская полиция может осуществить *революцию данных*.

Эта революция позволит:

- все шире и с хорошими результатами переходить от предотвращения к профилактике преступлений. В Соединенных Штатах уже появился соответствующий термин — *предикативная полицейская деятельность*;
- использовать информацию не только из полицейских баз, но и других государственных и частных баз, которые позволяют опережающим образом выявлять лиц и группы, уязвимые для преступников;

- *заранее распознавать подозрительные модели деятельности* и следы как готовящихся, так и уже совершенных преступлений. Наибольший эффект здесь может дать совмещение аналитики электронных платежей с видеоаналитикой и аналитикой совершаемых покупок;
- перевести дискуссии относительно уровня криминализации и уязвимости различных сфер деятельности, видов торговли и сегментов рынка с общетеоретического, экспертного анализа на язык документированной статистики. Выяснение тенденций, куда криминал направляет свои основные усилия, позволит британской полиции опережающе реагировать на изменение обстановки;
- *усилить контроль над полицией* со стороны общества — наряду с повышением уровня раскрываемости преступлений и все большим переносом работы с расследования на профилактику и предупреждение криминальных действий. В последние годы в парламенте Британии неоднократно поднимался вопрос о том, что *полиция отказывается открывать уголовные дела, связанные с высокими технологиями, гораздо чаще, чем в отношении других видов преступлений*. Использование данных и цифровых доказательств позволит и эту тему перевести из разряда экспертных дискуссий на уровень количественного анализа. Со временем контролирующие органы как внутри полиции, так и вне ее, смогут *в автоматизированном режиме выявлять все случаи необоснованного отказа в возбуждении уголовных дел, связанных с использованием высоких технологий*.

Лондонская, манчестерская, ливерпульская полиция, полицейские силы Глазго, Эдинбурга и Белфаста уже начали применять пробные формы предикативной полицейской деятельности. В ситуации, когда в самой полиции не было специалистов необходимого уровня по аналитике данных, выход был найден в тесном сотрудничестве с лучшими британскими университетами. Во взаимодействии с университетскими исследовательскими группами полиция этих городов сумела выйти на достаточно высокий уровень прогнозирования риска «традиционных преступлений», таких как кража со взломом, по отдельным районам городов вплоть до кварталов, а иногда и домов. После того как на основе данных предикативного анализа полицейские городские структуры изменили графики и распределение патрульных экипажей, удалось в течение 2015–2016 гг. добиться снижения преступности, эквивалентного снижению традиционной преступности, связанной с кражами со взломом суммарно за предыдущие семь лет. Эти результаты произвели огромное впечатление, как на полицейские силы, так и на население и бизнес. Полицейские перестали бояться высоких технологий, а бизнес стал охотнее жертвовать средства на повышение технического уровня полиции.

Это только первые шаги. Планируется сделать гораздо больше, чтобы в полной мере реализовать потенциал данных и аналитику данных в борьбе

с преступностью и ее профилактике. При наличии надлежащих гарантий в отношении личной информации необходимо помочь полицейским силам использовать данные так же легко, как сегодня британские интернет-магазины используют данные покупателей для таргетированной работы с клиентами. Вот почему руководство британской полиции:

- неуклонно выполняет *Национальную программу развития баз данных правоохранительных органов*. В рамках программы создается единая платформа, позволяющая одновременно централизовать данные, получаемые из национальной базы данных полиции, национальной базы компьютерной безопасности, национальной базы распознавания номеров и иных национальных и региональных баз, с возможностью обращения к этой базе всех полицейских подразделений и команд вплоть до патрульных экипажей. Когда платформа заработает на полную мощность, все британские полицейские смогут получать необходимую информацию в полном объеме в онлайн-режиме, в удобном и доступном для практического использования виде. Это не будет базой данных на уровне центрального аппарата министерства, это не будет базой данных лондонской полиции, *это будет база данных каждого полицейского Великобритании*;
- работает с Национальным советом начальников полицейских подразделений. Эта работа имеет своей главной целью обеспечить защиту населения и бизнеса от преступников, использующих высокие технологии не только для осуществления коммуникаций, но и для совершения преступных актов. В рамках этого станут более открытыми тендеры и конкурсы на поставку полиции самых эффективных решений;
- укрепляет связи с британскими и международными компаниями, специализирующимися на информационных технологиях и ориентированными на удовлетворение нужд полиции. В этих рамках завершается работа *по созданию единого стандарта технических и программных требований к информационно-коммуникационным компонентам, используемым полицией*. Создание подобного стандарта позволит британской полиции в рамках политики единой платформы расширить круг поставщиков и обеспечить большую эффективность при меньших затратах;
- уделяет особое внимание *опережающему созданию базы и аналитики данных, связанных с миграцией и предоставлением убежища*. В настоящее время основной упор в этой работе делается на обеспечение эффективной оперативной связи с пограничными службами и миграционными бюро. В Великобритании создается *единая база лиц, пересекающих границы Великобритании*. Соответственно, эта база будет включать *профили различного информационного объема в зависимости от продолжительности и целей пребывания иностранцев в Великобритании*. Специальный раздел этой базы, создаваемый в первую очередь, касается *нелегальных мигрантов*. По каждому выявленному случаю

будет собираться и храниться в базе максимум возможной информации. Есть основания полагать, что это позволит достаточно быстро *выявить конкретные преступные группы, обеспечивающие нелегальную миграцию в Великобританию*, и пресечь их деятельность. Именно это является наиболее эффективным подходом борьбы с нелегальной миграцией.

Использование существующих технологий и сканирование перспективных технологий, способствующих предотвращению преступлений

Министерство внутренних дел активно сотрудничает с правоохранительными органами и бизнесом в целях наиболее эффективного использования существующих технологий для предупреждения и борьбы с преступностью. Основными направлениями работы являются:

- **технологии цифровых расследований и разведки**. Цифровые источники играют все более важную роль в любом полицейском расследовании. Особо большие возможности предоставляет полицейским *разведка по открытым источникам, в первую очередь по социальным сетям и приложениям*. В условиях снижения возраста преступности, в том числе повседневной, уличной, практически весь криминал активно пользуется техническими устройствами. *Использование методов цифровой криминалистики*, например извлечение данных из захваченных в ходе расследований ноутбуков или смартфонов, позволяет получить результаты, на которые раньше, в доцифровом мире, у полицейских уходили недели упорной работы. Для того чтобы предоставить возможность полиции не просто в полной мере использовать указанные выше направления, но и применять собранные в ходе разведки по открытым источникам и цифровой криминалистики доказательства в суде, изобличающие преступников, необходимо дальнейшее совершенствование законодательства. Начиная с 2017 г. Министерство внутренних дел приступает к реализации программы «Цифровые расследования и разведка». Эта программа, наряду с усилиями по созданию единой платформы, поощряет овладение полицейскими методами разведки по открытым источникам и цифровыми расследованиями и оснащение их простым, но эффективным софтом;
- **технологии судебно-медицинской экспертизы**. Судебно- медицинская экспертиза — это криминалистические наука и практика, связанные с расследованием места преступления и анализом собранных доказательств. Переход общества в цифровой мир создал принципиально новые, гораздо более широкие, чем раньше, возможности для проведения экспертизы. Виртуальная реальность, в отличие от реальной, хранит больше следов и гораздо дольше. Соответственно, при необходимом оснащении это повышает вероятность правильно установить преступника и задержать его. Министерство внутренних дел осуществляет программу «Цифровые судебно-медицинские

расследования». Эта программа подкреплена финансами и способствует не только повышению уровня оснащения лабораторий по проведению экспертизы, но и привлечению в полицию специалистов по цифровым расследованиям, а также по использованию новых методов судебно-медицинской экспертизы;

- **мобильные технологии**. Министерство внутренних дел создает в сотрудничестве с британским бизнесом единую систему связи для аварийных служб, включая полицию, пожарно-спасательную службу и скорую медицинскую помощь. Также эта система будет подключена к отдельным бизнес-структурам и общественным организациям. В 2018 г. в Великобритании уже создана единая сеть аварийных служб. Она обеспечит надежные услуги голосовой, текстовой и широкополосной видеосвязи, включая передачу данных. Система, располагающая мощнейшими центрами обработки данных, будет выведена на смартфоны, а также специальные устройства, прикрепленные к амуниции работников аварийных служб. Соответственно, работники аварийных служб, находящиеся на переднем крае, в какой бы критической ситуации ни оказались, смогут не только поддерживать связь, но и оперативно получать необходимую помощь;
- **технологии цифрового видео**. Британская полиция видит три основных направления использования цифрового видео в своей деятельности. Во-первых, *видеоматериалы с места преступления*. Во-вторых, *канал взаимодействия с общественностью*. В-третьих, гигантский, пополняемый в онлайн-режиме *видеоархив с камер наблюдения в британских городах и на транспортных магистралях*. Впервые в истории у британской полиции есть в распоряжении программно-аппаратные средства, позволяющие в онлайн-режиме работать с *потоковым многоканальным видео*. По сути, речь идет о том, что впервые у полиции появляется возможность предикативно анализировать намерения потенциальных преступников, а также фиксировать на пленку уже совершенные преступления либо обнаруживать скрывающихся преступников. Главной проблемой на сегодняшний день являются уже не программно-аппаратные средства, а *внесение изменений в британское законодательство, чтобы видеоматериалы могли рассматриваться как доказательства в процессе уголовного производства*.

Перспективные направления

В Министерстве внутренних дел Великобритании был создан *Центр перспективных прикладных наук и технологий (CAST)*. Его задачей является работа с бизнесом и наукой по выявлению новых технологий и при необходимости их финансовая и иная поддержка. Особое внимание Центр уделяет не международным и ведущим британским компаниям-поставщикам Министерства внутренних дел, а исследовательским командам в британских университетах, стартапам и т.п. Центр не только внимательно изучает их разработки, но

и облегчает доступ лучшим из них к тендерам, проводимым Министерством внутренних дел.

В рамках работы Центра наряду с традиционными направлениями особое внимание уделяется таким перспективным технологиям, как:

- **3D- и 4D-печать**. Трехмерная печать позволяет создавать объекты при помощи послойного нанесения материала в определенной форме. 4D-печать представляет собой 3D-печать, чья форма программируемо изменяется с течением времени. Первое оборудование для 4D-печати уже создано в британских университетах. Данная технология интересна для Центра с позиции возможности использования 3D- и 4D-печати преступниками. Если пластиковые пушки в настоящее время ненадежны и представляют большую угрозу для стрелка, чем для жертвы, то стремительно развивающаяся 3D-печать из металла позволит преступникам оснащать себя стрелковым оружием прямо дома — с низкими затратами и высоким качеством. Благодаря тому, что удалось своевременно распознать эту угрозу, в настоящее время в Великобритании компании, производящие 3D-принтеры для металлической печати, получают специальную разрешительную лицензию, которая предусматривает не только предоставление МВД сведений обо всех покупателях подобных устройств, но и установку внутрь устройств вшитых распознавателей локации. Также удалось выявить такие угрозы, как применение 3D-печати в производстве различных устройств, используемых для контрабанды наркотиков, произведений искусства и т.п.;
- **дроны**. Нынешние разработки в области робототехники позволяют массово производить летающие роботы, несущие полезную нагрузку до 25 кг, со временем полета более 2 часов и скоростью до 400 км/ч, по цене 200–300 фунтов стерлингов. Очевидно, что подобные дроны, используемые в настоящее время в основном государственными службами, в ближайшие год-два станут оснащением преступников. Центром совместно с лабораториями в Саутгемптонском и Бристольском университетах удалось создать устройство, которое позволяет распознавать на высоте до 1,5 км характер груза, перемещаемого на дроне, идентифицировать основные виды взрывчатки, наркотиков и химических реагентов. Эта революционная разработка позволит сбивать или сажать путем перехвата управления подобные преступные дроны;
- **биткоин- и блокчейн-технологии**. Биткоин — это одна из виртуальных валют. Если на первом этапе биткоины вызывали большие подозрения у правоохранительных органов, то сегодня ситуация изменилась. Британское Министерство внутренних дел четко разделяет анонимные виртуальные криптовалюты, использование которых запрещено, и технологии блокчейна. Если анонимные виртуальные валюты являются все более важным платежным средством для различного рода незаконных транзакций — от оплаты убийств, наркотиков и т.п. до вывода за рубеж коррупционных и прочих нелегальных денег,— то

технологии блокчейна осуществляют революцию в финансах. Великобритания наряду с Соединенными Штатами является лидером использования блокчейн-технологий в финансовом секторе. Для того чтобы разобраться во всех аспектах блокчейн-технологий, Министерство внутренних дел ассигновало Центру и Институту Алана Тьюринга по 10 млн. фунтов стерлингов ежегодно (вплоть до 2020 г.) на блокчейн-исследования;

- **всеобщая взаимосвязь**. В настоящее время мир движется к сплошной связанной среде и инфраструктуре. К 2020 г. в мире будет около 20 млрд. связанных между собой сетевых устройств. Министерство внутренних дел понимает, что глобальный связанный мир сильно изменяет требования к работе правоохранительных органов. В полностью связанном мире криминал, не ограниченный законодательством, будет действовать глобально, поверх государственных границ. В то же время правоохранительные органы в своих действиях ограничены государственной юрисдикцией. Если эта проблема до 2020 г. не будет разрешена, то преступники получат огромное, а возможно, решающее преимущество. Несмотря на надежды руководителей отдельных крупных государств на эффективное закрытие собственного информационного пространства, это технически невозможно на программно-аппаратном уровне. Кроме того, любые подобные попытки приведут к отрыву государства от мировой экономики и глобальной технологической гонки и в конечном итоге к его стремительной деградации. Поэтому Министерство внутренних дел исходит из концепции открытого глобального связанного пространства и предлагает искать пути решения этой острейшей, неосознаваемой обществом на сегодняшний день проблемы различными способами, в том числе нетрадиционными. Например, возможно *выделить цифровую среду в особый тип среды, в которой будут действовать законы, отличные от наземной, воздушной или водной сред*. Такой подход еще более 50 лет назад в расколотом на блоки мире был применен для правового регулирования космического пространства;
- **цифровое шифрование**. Цифровое шифрование амбивалентно. С одной стороны, оно создает возможности для общественности, граждан и бизнеса защитить свою информацию не только от преступников, но и от несанкционированного доступа к ней правительственных структур. С другой стороны, широкое распространение шифрования создает большие трудности для полицейских органов. Начиная с 2013 г. многие британские граждане стали использовать шифрованную электронную почту, мессенджеры и т.п. Это создает значительные затруднения правоохранительным органам. Вероятно, необходимо регламентировать возможности шифрования гражданами, а также специально предусмотреть обязанность для производителей шифрованных коммуникаторов предоставлять соответствующие ключи правоохранительным органам.

Помимо изучения конкретных технологий, Центр уделяет особое внимание изучению вопроса: как новые технологии будут взаимодействовать и влиять друг на друга. Центр будет выпускать ежегодный доклад по перспективным тенденциям развития технологий с точки зрения полиции. Такой доклад позволит не только использовать потенциал технологической революции для повышения эффективности работы полиции, но и своевременно оценить риски и угрозы попадания этих технологий в руки криминала.

Искусственный интеллект и большие данные для предупреждения и раскрытия преступлений

Искусственный интеллект

Джошуа Бенджо, профессор информатики в Монреальском университете, один из пионеров в области разработки методов глубинного обучения, считает, что после 2005 г. исследования в области искусственного интеллекта стали перспективным делом. И произошло все это благодаря **концепции глубинного обучения** — так называется подход к созданию компьютеров, наделенных искусственным интеллектом, черпающий вдохновение в нейробиологии. В последние годы концепция глубинного обучения стала тем самым локомотивом, который придал ускорение исследованиям в области искусственного интеллекта. Теперь крупнейшие ИТ-компании принялись вкладывать в технологию глубинного обучения миллиарды долларов («В мире науки» [08/09], август/сентябрь 2016).

Принцип глубинного обучения заключается в моделировании нейронных сетей, которые постепенно учатся распознавать изображения, понимать речь и даже самостоятельно принимать решения. Технология глубинного обучения основана на использовании так называемых искусственных нейронных сетей — основного объекта нынешних исследований в области ИИ. Нет, виртуальные, искусственные нейронные сети вовсе не представляют собой точную копию настоящих нейросетей головного мозга, и функционируют они примитивнее: в основу их работы положены общие математические принципы обучения на примерах из обучающей выборки, что позволяет нейросетям распознавать всевозможные объекты на фотографиях (например, лица людей и т.д.) или переводить тексты, написанные на основных языках мира.

Технология глубинного обучения коренным образом изменила сам характер исследований в области ИИ, вдохнув новую жизнь в позабытые было амбициозные планы по созданию компьютерного зрения, распознаванию речи, обработке естественных языков, реализации проектов в области робототехники. Первые программы распознавания речи были созданы в 2012 г. (например, всем известный сервис Google Now). Затем стали появляться приложения, распознающие фотографии (данная функция в настоящее время интегрирована в сервис Google Photos).

До недавнего времени искусственные нейронные сети использовались в значительной степени для распознавания статичных образов. Однако постепенно получил известность и другой тип нейросетей — **рекуррентные нейронные сети**, которые стали применяться в основном для анализа процессов, протекающих во времени. В частности, такие сети оказались способны корректно выполнять обработку аудио- и видеоизображений, а также некоторых других видов информации. Последовательные данные состоят из блоков (фонем, слов), которые следуют друг за другом. Процесс обработки входных сигналов с помощью рекуррентных нейросетей имеет сходство с работой мозга, ведь и в головном мозге во время обработки информации, поступающей от органов чувств, происходит постоянное изменение сигналов, циркулирующих между нейронами. Получается, что состояние каждого нейрона во внутренних слоях постоянно меняется в зависимости от мощности сигналов, поступающих в головной мозг из внешней среды, а на выходе мы получаем последовательность команд, которые инициируют двигательную активность разных частей тела, направленную на достижение конкретной цели.

Рекуррентные нейронные сети способны предсказывать, например, каким будет следующее слово в предложении, а это слово, в свою очередь, тоже может использоваться для генерирования новых последовательностей слов. Кроме того, с помощью рекуррентных нейронных сетей можно решать и более сложные задачи.

Нейросети могут использовать временную память компьютера для обработки нескольких рассредоточенных кусков информации (например, идеи, содержащиеся в различных предложениях, разбросанных по документу).

Дэвид Кроуфорд, директор по разработке программного обеспечения в компании Alation, которая занимается каталогизацией данных, полагает, что сейчас по-прежнему существуют области, где алгоритмы нуждаются в людях. *Искусственный интеллект может работать только в тех сферах деятельности, которые человек может точно описать*.

Работа аналитика выходит за рамки проведения анализа в закрытой среде. Анализ должен быть применен к внешнему миру, где контекст влияет на интерпретацию результатов.

Маловероятно, что в ближайшее время алгоритмы научатся понимать людей. Этого не случится, пока человечеству не удастся улучшить интерфейсы взаимодействия мозга человека и компьютера.

Будущее аналитиков менее мрачно, чем об этом говорится в заголовках СМИ. Достижения в области ИИ во многом напоминают эффективных помощников, а не замену аналитикам. В будущем аналитики получат группу алгоритмов с ИИ, которые будут проводить анализ данных. Задача аналитиков будет состоять в том, чтобы указать ИИ на правильные вопросы для анализа и решить, как применять результаты анализа для решения проблем в реальном мире. *Пока конечный потребитель аналитики — человек, аналитики никуда не денутся.*

Лидером внедрения искусственного интеллекта в процесс борьбы с преступностью является ФБР США. Основные работы в этом направлении ведутся в Информационном центре ФБР (NCIC).

NCIC — это метабаза, включающая на начало 2017 г. 21 базу данных, содержащую досье на 12 млн. активных индивидуальных преступников и членов преступных организаций. NCIC в среднем отвечает на 14 млн. запросов в день. Помимо ФБР, NCIC обслуживает более 90 тыс. точек доступа в органах уголовного правосудия, а также судах, прокуратуре, системе исправительных учреждений и т.п.

Информационный центр ФБР находится в состоянии модернизации, известной как проект «N3G». В рамках проекта в систему включаются принципиально новые блоки обработки и анализа информации, базирующиеся на **интеллектуальном анализе больших данных**. В 2017 г. началось **сооружение и оснащение здания нового Центра данных и вычислений взамен действующего**.

Новый Центр будет запущен в рамках проекта «N4G». По площади он будет в 12 раз превосходить действующий в настоящее время Центр в Бриджпорте (штат Коннектикут) и **иметь более чем в 50 раз большие емкость хранения и мощность обработки данных**. Предусматривается, что Центр будет подключен к национальной сети суперкомпьютеров АНБ и Министерства энергетики. Программно-аппаратная архитектура Центра проектируется вокруг **программно-аппаратных комплексов искусственного интеллекта**.

Работы ведутся совместно с Лабораторией искусственного интеллекта корпорации Google.

Особое внимание ФБР уделяет **скачкообразному увеличению быстродействия компьютеров**. От многих из нас укрылось определяющее обстоятельство. Выигрыш у человека в го был осуществлен не просто компьютером Google, а программно-аппаратным комплексом, где за программу отвечали алгоритмисты Google, а железо сделала канадская компания, недавно купленная Google — Google DeepMind. DeepMind — это единственная сегодня компания в мире, которой удалось создать действующий квазиквантовый компьютер. Квази — потому, что значительная часть вычислений осуществляется в рамках традиционного кремниевого электромеханического компьютера, и лишь некоторые выполняет квантовый компонент. Но даже в таком виде **обеспечивается на порядок более высокая скорость, чем у современных кремниевых суперкомпьютеров.** Чем выше скорость, тем проще осуществлять глубокое обучение методом проб и ошибок.

Основные направления применения искусственного интеллекта в структуре ФБР и полиции США в 2017–2020 гг.

Двусторонние и многосторонние встречи, открытые конференции и совещания за закрытыми дверями позволили определить основные направления использования искусственного интеллекта и его элементов в работе ФБР

и полиции штатов. Эти направления нашли отражение в концепции «N4G». В число основных направлений включаются:

1. Использование в аналитико-ситуационных центрах в офисах ФБР на местах и в аналогичных офисах полиции штатов программно-аппаратной среды с единой интегральной обработкой файлов различной размерности и формы представления, включая текстовые, табличные, аудио- и видеофайлы, сигнальные файлы от датчиков, банковские транзакции, показания локации и т.п.

До конца 2017 г. минимум в пяти полицейских управлениях на уровне штатов и в двух отделах ФБР будут запущены подобные пилотные ситуационные центры.

2. В настоящее время ФБР и полиция подвергаются частично оправданной критике за хранение избыточной информации об американцах. Например, в 2016 г. в Конгрессе США рассматривался доклад Центра по конфиденциальности и технологиям Университета Джорджтауна. В ходе дискуссий по докладу выяснилось, что в настоящее время в базе данных ФБР и полиции содержатся биометрические данные 130 млн. американцев, т.е. более половины взрослого населения страны. В ходе обмена мнениями стороны согласились, что порядка 35 млн. единиц хранения являются избыточными, поскольку эти люди никогда не совершали противоправных поступков, не имели связей и отношений с террористами и преступниками, а также не совершали предосудительных поступков в общественном плане. На этом совещании представитель ФБР был вынужден признать, что в базе не оказалось примерно 1,5 млн. единиц хранения биометрических данных тех американцев, которые впервые совершили преступления в период 2010–2015 гг. *(Полные профили, включающие до 50 параметров, содержатся на 12 млн. американцев; в то же время на 130 млн. американцев в базе ФБР содержатся фотографии, голосовые данные и т.п. Они не считаются полным профилем и не составляют индивидуальный идентификационный файл гражданина.)*

Данная ситуация сложилась не из-за злого умысла или стремления ФБР играть роль Большого Брата, а из-за способа ввода биометрических данных и особенностей их хранения. Сегодня Информационный центр ФБР и локальные информационные центры полиции штатов вводят биометрические данные вручную в соответствии с решениями, принимаемыми людьми. Кроме того, хотя ФБР и использует наиболее современные на сегодняшний день технические средства, они предусматривают отдельное хранение и обработку биометрических данных.

Для преодоления этих недостатков с 2015 г. Центр ФБР совместно с MTI и Google ведет работу по созданию **рекуррентной базы данных**. По предварительным подсчетам, в течение 2017 г. база будет запущена в опытную эксплуатацию. Ее принципиальное отличие от ныне существующих баз данных состоит из трех моментов. **Не человек, а машина будет принимать решение о появлении того или иного профиля в базе данных**. Грубо говоря, предусматривается

система, в корне отличающаяся от ныне принятого порядка. Сейчас соответствующие руководители полиции, агенты ФБР принимают решения о заведении файлов на того или иного человека. Как показывает практика, эти решения часто бывают ошибочны и субъективны. Новую же систему предполагается обеспечивать нефильтрованными потоками информации. Фильтровать, а соответственно, определять необходимость заведения профилей будет сама система. В систему встраивается модуль глубокообучаемых нейронных сетей. Данный модуль будет отвечать за своевременное исключение профилей и параметров лиц, которые по критериям базы попали в нее, но в течение определенного времени не вызвали интереса со стороны ФБР или полиции штатов. Наконец, данная система, в отличие от ныне применяемых, будет способна взаимодействовать с конечными пользователями на естественном языке и с использованием визуальных средств.

3. Как уже отмечалось, одним из наиболее угрожающих с точки зрения динамики организованной преступности секторов экономической жизни страны являются небанковские платежные системы. По согласованию с наиболее динамичными платежными системами Stripe и Wise ФБР организовало **частно-государственное партнерство по созданию и эксплуатации платформы по обнаружению мошенничеств и взломов платежных систем**. Данная система будет открыта для всех лицензированных платежных систем. Предусматривается, что они будут выделять на содержание системы ежегодный взнос в зависимости от объема транзакций и уровня сертификата информационной защиты, присвоенного платежной системе. Производителем системы в результате тендера выбрана компания Palantir. В 2017 г. она должна запустить платформу POLPAY.

4. В 2017 г., используя платформу контекстного интеллекта Nigel, предусматривается создать **безбумажный офис агента ФБР или полицейского участка**. Поскольку система Nigel, в отличие от других, способна не только к семантическому анализу *(распознаванию объектов по различным онтологиям: свойства, отношения, функции, человек, юридическое лицо, предмет и т.п.)*, но и к контекстному распознаванию ситуации *(ситуации могут быть одинаковыми по онтологиям, но различными по смыслу. Например, в двух ситуациях участвуют одни и те же персонажи: женщина, мужчина и ребенок. Контекст ситуации может быть различным: одном случае это будет счастливая семья, в другом — бывшие супруги, делящие ребенка. Сейчас ни одна система, кроме Nigel, не способна распознавать ситуацию)*, она будет давать экспертные советы правоохранителям, привязанные к уникальной, конкретной обстановке.

5. **Использование искусственного интеллекта для экономии бюджета ФБР и полиции штатов**. В настоящее время почти четверть работников, которые проходят как занятые в полиции штатов и на которых приходится чуть больше 15% фонда заработной платы, заняты различного рода рутинными операциями, имеющими общепрофессиональный характер. Речь идет о многочисленных

секретарях, юрисконсультах, фотографах и т.п. **В течение 2017–2020 гг. в рамках программы сокращения бюджета федеральных органов власти за счет роботизации ФБР будет последовательно заменять юрисконсультов и секретарей роботизированными устройствами**. В настоящее время для ФБР на 2020 г. установлен норматив сокращения не менее 10% вспомогательного персонала, не связанного с выполнением оперативно-разыскных, следовательских и других полицейских функций, а также работой в лабораториях.

6. Начиная с 2017 г. ФБР совместно с компанией ForAllSecure и Университетом штата Пенсильвания приступило к разработке **системы Mayhem — первой в мире системы искусственного интеллекта, основными функциями которой являются распознавание индивидуального почерка хакеров и хакерских группировок, а также обнаружение атак и активного тестирования и преследование хакеров в их ходе, вплоть до установления их локации**.

ФБР и исследователям из Пенсильванского университета удалось установить, что методы комбинаторики позволяют системам искусственного интеллекта распознавать в доли секунды некоторые особенности вредоносного софта, а также архитектуры атак, которые из-за недостатка времени укрываются от высококвалифицированного персонала служб информационной безопасности.

Есть основания полагать, что данная система является подлинным прорывом и может обеспечить долгожданный перелом в состязании информационных меча и щита.

Большие данные против криминала

Как отмечают исследователи больших данных, сам термин «большие данные» (Big Data) не имеет общепринятого определения даже в индустрии информационных технологий. Наиболее распространенным является раскрытие феномена больших данных через указание проблем, с которыми приходится сталкиваться на современном этапе развития технологий при обработке информации. Исходя из этого, большие данные определяются посредством указания следующих основных характеристик: 1) большого объема, 2) разнообразия данных, 3) высокой скорости их изменения.

Согласно указанному подходу, помимо собственно обработки больших объемов данных, проблема, решаемая посредством Big Data, состоит также и в том, что большая часть потенциально ценной информации представлена в неструктурированном виде, то есть не упорядочена и содержится в различных форматах, в отличие от сведений, наполняющих традиционные базы данных. Огромные массивы разнообразной информации, например информация с форумов и из социальных сетей, видеозаписи, текстовые документы, лог-файлы или данные о трафике и соединениях абонентов, содержатся в различных источниках, нередко за пределами организации. В результате правоохранительные структуры могут иметь доступ к огромному объему данных из внутренних и внешних

источников, но не обладать необходимыми инструментами, чтобы осуществить их совместную обработку, выявив определенные взаимосвязи, и сделать на их основе значимые выводы. *Технологии больших данных позволяют решить эту проблему, связав воедино разнородные данные*.

Другой признак больших данных состоит в том, что обрабатываемая с использованием указанной технологии информация обновляется быстро (например, «потоковые данные»), при этом необходимо принимать решения на основании ее оперативного анализа.

Анализируя различные зарубежные подходы, российский исследователь А. И. Савельев определяет большие данные как *совокупность инструментов и методов обработки огромных объемов структурированных и неструктурированных данных из различных источников, подверженных постоянным обновлениям, в целях повышения качества принятия управленческих решений, создания новых продуктов*.

Опыт сотрудничества **IBM** с правоохранительными органами свидетельствует о том, что требуется, во-первых, консолидация разрозненных источников информации в единое хранилище данных; во-вторых, применение специального ПО, позволяющего выявлять полезную информацию из нецелостных и неполных документированных данных, а также из несвязанных событий; в-третьих, использование специализированных программно-аппаратных решений, максимально ускоряющих работу и принятие решений при обработке огромных объемов структурированной и неструктурированной информации.

Например, с этой целью в **Нью-Йорке** в 2007 г. было решено создать **централизованный операционный центр общественной безопасности**. Было интегрировано более 100 разрозненных источников данных. Все потоки информации от патрульных машин, тысяч камер видеонаблюдения, звонки от свидетелей в виде неструктурированных данных поступают на корпоративную шину данных и преобразуются в универсальный формат. Затем аналитические инструменты ассоциируют информацию, помещая ее в определенный контекст, и распределяют ее согласно запросам пользователей. Аналитическая система ассоциирования распознает не только структуру, но и значение информации, включая взаимоотношения между различными частями. Создание единого хранилища позволило снизить преступность в городе на 27%.

Был реализован также сервис поиска полезных данных из плохо документированной информации: жалоб граждан, отчетов полиции, записей на номер 911, протоколов арестов и др. Все эти данные изобилуют неточностями, сокращениями, аббревиатурами, специальными терминами и т.п., и выявление нужных сведений и взаимосвязей при помощи традиционного контекстного поиска в них крайне затруднительно.

В результате удалось достичь общего повышения эффективности работы. Применение инструментария поиска и анализа позволило сформировать

описание событий, классифицировать их (при этом поиск осуществляется по неструктурированной информации, содержащей порой неточные описания). В первые недели эксплуатации системы на основании данных отчетов было раскрыто несколько старых дел по убийствам.

В целом это позволяет создать простые унифицированные представления для каждого аспекта работы полиции, включая планирование, отчетность и совместную работу.

Ключевыми элементами работы операционного центра полиции Нью-Йорка является пространственно-временная модель города и поведенческие модели, которые используются для связывания наиболее вероятных сценариев для криминалистов. *Центр по раскрытию преступлений реального времени (RTCC)* использует ситуативный подход к большим данным, который требует особых навыков для составления запросов и интерпретации извлекаемых знаний. В результате каждое обращение к большим данным является уникальным поиском, в отличие от стандартных систем анализа информации в транзакционных и других системах управления реляционными базами данных с их фиксированными запросами и типовыми задачами.

Свою эффективность доказала система Blue CRUSH (от англ. Crime Reduction Utilizing Statistical History — *«снижение преступности на основе статистических данных»*), разработанная **компанией IBM**, которая поставляет полицейским подготовленные на основе имеющейся статистики совершения преступлений сведения о зонах потенциальной угрозы совершения преступления с указанием места (в пределах нескольких кварталов) и времени (в пределах нескольких часов конкретного дня недели). Подобного рода профилактическое прогнозирование привело к снижению уровня преступности в *городе Мемфисе* на 31%, из которых 15% приходится на тяжкие преступления.

Благодаря расширенному использованию информационных технологий в борьбе с преступностью и чрезвычайными обстоятельствами, стало возможным:

- реализовать автоматический анализ видеоинформации для предотвращения преступлений;
- ускорить расследование преступлений в 10–30 раз;
- использовать автоматизированные предсказания, поиск ассоциативных связей и техники кластеризации данных для ускорения принятия решений;
- автоматизировать процесс построения регламентов ответа на чрезвычайные ситуации;
- обеспечить сопровождение событий и отображение местонахождения сил и средств в реальном времени.

В 2001 году IBM приобрела британскую компанию i2 Group, которая разрабатывала аналитические средства для правоохранительных органов, спецслужб, военной разведки и специалистов по борьбе с фродом.

Один из продуктов, основанных на i2,— специально для полиции. Он позволяет быстро получить доступ к информации, накопленной американскими правоохранительными органами, и проявить в ней **скрытые связи между людьми, местами, автомобилями, мобильными телефонами и тому подобными объектами**.

В 2007 году полиция *Северной Каролины* начала использовать средства i2 для анализа своего архива данных о преступности. За четыре года в одном из районов количество совершаемых преступлений удалось сократить на 50%. Вряд ли такой прогресс объясняется исключительно силой софта IBM, но и его вклад никто не отрицает.

В канадском *Ванкувере* полиция внедрила систему анализа данных, основанную на разработках IBM и географической информационной системе Esri. Система не только выявляла тенденции, но и предсказывала вероятное время и место совершения преступлений. С 2007 по 2011 г. количество преступлений, связанных с собственностью, сократилось на 24%, а насильственная преступность — на 9%.

Похожие результаты сообщают полицейские департаменты Лас-Вегаса, Мемфиса и других городов, где экспериментируют с программами для анализа данных.

В полиции *Лос-Анджелеса* компьютерный алгоритм занимается тем, что обычно называют **проактивной правоохраной**. Используя отчеты о преступлениях за годы и десятилетия, алгоритм определяет районы, где вероятность совершения правонарушений является наибольшей. Он отмечает такие участки на карте города небольшими красными квадратами, и эти данные тут же передаются в патрульные машины.

Система прогнозирования преступлений, разработанная в *лос-анджелесском кампусе Калифорнийского университета (UCLA)*, теперь известна под названием *PredPol* и стоит на балансе десятков полицейских подразделений.

В 2014 г. PredPol применялась в 7 территориальных подразделениях полиции Лос-Анджелеса. Их патрули оснащены электронными картами с десятками мигающих красных квадратов, которые указывают места возможной противоправной деятельности. Полиция Лос-Анджелеса сосредоточила силы на кражах имущества из домов и машин и угонах — видах преступлений, составляющих более половины из 104 тыс. правонарушений, случившихся за 2014 г. в городе.

Десятки других населенных пунктов по всем Соединенным Штатам и за их пределами используют программное обеспечение PredPol для прогнозирования других преступлений, включая активность организованных преступных группировок, наркоторговлю и незаконное применение огнестрельного оружия. Полиция *Атланты* применяет PredPol для прогнозирования грабежей и разбоев. В *Сиэтле* она используется для прогнозирования вооруженного насилия. В *Кенте* (Англия) PredPol применялась для предсказания наркопреступлений и грабежей. Полиция Кента была еще более изобретательной: не только отправляла своих сотрудников патрулировать опасные районы, но также прибегала

к помощи местных волонтеров-дружинников и работников реабилитационных клиник для наркоманов.

Система прогнозирования в режиме реального времени анализирует новые отчеты о преступлениях в этих городах, и красный квадрат, предсказывающий место совершения правонарушения, может сдвинуться в любой момент. Хотя патрульные из подразделений, использующих PredPol, обязаны находиться определенное количество времени в каждом из тех красных квадратов, они не просто слепо следуют командам системы. Патрульный вправе принимать решения самостоятельно, исходя из обстановки, а не только подчиняясь алгоритмам.

Использование больших объемов данных и обработка с помощью математических моделей значительно превосходит по конечному результату банальное определение «горячих точек» на карте в ручном или даже автоматизированном режиме. Специальные испытания, проводившиеся почти 2 года в трех территориальных подразделениях лос-анджелесской полиции, установили, что PredPol верно предугадывает в 2 раза больше мест преступлений, чем позволяют существующие методики из числа лучших.

Специальное программное обеспечение применяется *полицией Чикаго*. Оно с высокой вероятностью предсказывает не только имена будущих убийц, но и тех, кто станет жертвами,— в американской преступной среде эти категории людей плотно пересекаются.

Программа, разработанная при участии ученых из *Иллинойского технологического университета (США)* (разработчик — профессор Майлз Веркик), позволила полиции Чикаго определить список лиц, находящихся в группе риска совершения убийств. Узнав их имена, полицейские ведут с ними профилактическую работу, предположительно позволяющую снизить вероятность посягательств на жизнь других людей.

В основе работы программы лежит отбор по десяти основным признакам. Среди них есть ряд цифр по истории приводов того или иного лица в полицию. Среди прочего алгоритм учитывает, были ли у человека аресты за незаконное ношение огнестрельного оружия или за участие в структурах организованной преступности. Алгоритм ищет людей, которые соответствуют всем или хотя бы нескольким критериям отбора. Те, кто набирает больше всего пересечений по списку критериев, вносятся в группу максимального риска.

По заявлениям полиции, новый алгоритм является довольно эффективным. Из 2,7 млн. жителей Чикаго программа отобрала лишь 1400 человек, имеющих чрезвычайно высокую вероятность убить или быть убитым. Более 70% человек из данного списка были застрелены в течение 2016 г. Каждый 4-й стрелок также входил в список Департамента полиции Чикаго. Согласно данным правоохранителей, 117 из 140 человек, арестованных во время общегородского рейда против банд, также присутствовали в вышеупомянутом перечне и составляли группу риска.

Полицейские применяют новый метод не только для своевременного совершения арестов. Власти города видят в алгоритме эффективное средство «*персональных уведомлений*»: когда работники социальной сферы и общественные лидеры агитируют членов-лидеров «списка стратегических субъектов» изменить образ жизни и навсегда покинуть криминальный мир.

Полиция города Дарема на севере Англии запустила в 2017 г. компьютерную программу, которая при помощи алгоритма искусственного интеллекта должна помочь полицейским *определить, кого следует содержать под стражей, а кого можно отпустить*. Алгоритм классифицирует задержанных по степени риска — с какой вероятностью они могут вновь совершить преступление.

Программа Harm Assessment Risk Tool (Hart) изучала данные полиции Дарема об арестах за период в пять лет, между 2008 и 2012 г. Затем система была протестирована даремской полицией в 2013 году, после чего в течение двух лет изучались результаты этого тестирования: полицейские отслеживали, вернулись освобожденные к преступной жизни или нет. Как выяснилось, алгоритм мог предсказать, что задержанный не представляет опасности, в 98% случаев. А находящихся в группе высокого риска компьютер правильно выявлял в 88% случаев. Это отражает настройки алгоритма искусственного интеллекта: он запрограммирован осторожничать и классифицировать задержанных людей чаще в группы среднего или высокого риска, чтобы не выпускать на свободу тех, кто может снова совершить преступление.

В ходе испытаний программы полицейские следили за выводами Hart, но вердикт алгоритма не влиял на принятие решения об аресте.

Подозреваемые, ранее не совершавшие преступлений, с меньшей вероятностью будут записаны алгоритмом искусственного интеллекта в категорию высокого риска. Однако если они арестованы по подозрению в серьезном преступлении, как, например, убийство, то это отразится на оценке программы.

Программа может быть хорошим помощником во многих случаях: когда полиции следует решить, держать ли задержанного еще несколько часов, следует ли отпустить его под залог до того, как ему будут предъявлены официальные обвинения, и стоит ли держать его под арестом после предъявления обвинений. В ходе нового эксперимента полицейские будут использовать систему при рассмотрении лишь ряда дел, выбранных случайным путем.

Любой вывод алгоритма носит лишь рекомендательный характер и ни в коем случае не отбирает у полиции прерогативу принимать окончательное решение о судьбе задержанного. Алгоритм должен сохранять все данные о том, как программа пришла к определенному выводу.

Кроме того, британская полиция с 2014 г. проверяет *компьютерную систему, которая поможет собрать воедино то, что могло произойти на месте преступления*. Идея состоит в том, что система, называемая VALCRI, будет в течение нескольких секунд выполнять кропотливую работу аналитика, освобождая

его для того, чтобы он мог сосредоточиться на деле, а также провоцируя новые направления расследования и возможные упущенные детали.

Основная работа VALCRI заключается в том, чтобы помочь генерировать правдоподобные идеи о том, как, когда и почему было совершено преступление и кто сделал это. Она сканирует миллионы полицейских записей, интервью, фотографий, видеороликов и многое другое, чтобы определить связи, которые, по ее мнению, имеют отношение к делу. Все это затем выводится на два больших сенсорных экрана для взаимодействия с аналитиком.

Мидлсекский университет является одним из нескольких высших учебных заведений, которые в данный момент задействованы в разработке системы VALCRI. Аббревиатура расшифровывается как Visual Analytics for sense-making in Criminal Intelligence analysis.

VALCRI исследует личные дела преступников и разделяет паттерны их поведения на отдельные категории. По почерку преступника система практически мгновенно предложит следователям несколько наиболее подходящих кандидатур, которые были бы способны совершить данное преступление. Причем информация будет предлагаться сотрудникам полиции в интуитивно понятном и очень удобном графическом интерфейсе.

Вместо того чтобы разделять преступников по категориям преступлений, таким как квартирные кражи или взлом автомобилей, VALCRI запоминает и анализирует паттерны поведения преступника, в данном случае — склонность к кражам. Таким образом, VALCRI решает проблему слабого сотрудничества полицейских подразделений, а также учит полицейских обращать внимание на ключевые детали преступления.

В целом ряде штатов США использование полицией методов и алгоритмов кластеризации и классификации технологии Text Mining (для выделения криминально значимой информации) совместно с технологией Visual Mining в режиме реального времени обеспечивает возможность выполнения аналитической работы по профилактике и расследованию преступлений в автоматизированном режиме на качественно новом уровне. Эта возможность реализована в интеллектуальной системе криминального анализа в реальном времени — Real-time Intelligence Crime Analytics System (RICAS), которая позволяет связать географическое положение, время, лица и события в одном визуальном пространстве отображения.

В основу построения системы положены следующие факторы:

- любая криминально значимая информация содержит данные о месте, что может быть отражено либо в текстовом формате в виде адреса, либо в географических координатах, и времени совершения преступного деяния;
- любой субъект или объект преступления имеет привязку к географическим координатам в текстовом формате (адрес прописки, проживания, места работы, регистрация предприятия, транспортного средства, оружия и т.д.);

- криминальные события, субъекты и объекты могут иметь взаимосвязи, которые легче обнаружить путем анализа визуального отображения в едином пространстве представления (на одной карте): например, если в месте совершения разбойного нападения проживают лица, ранее привлекавшиеся за аналогичные преступления, то существует большая вероятность совершения ими данного деяния;
- отображение в едином пространстве событий, растянутых во времени (происходящих в разное время), позволяет обнаружить скрытые закономерности визуально.

С учетом этих факторов в представляемой системе программно реализованы адаптированные алгоритмы технологий Data Mining, Text Mining, Visual Mining и Link Analyzes, которые обеспечивают выполнение следующих операций с потоками входных данных:

- кластеризация объектов по одному или нескольким признакам, имеющим общие пространственно-временные характеристики;
- создание временной ленты событий для определенного географического места (ретроспективный анализ криминальных событий, произошедших в заданный период времени в районе места исследуемого происшествия);
- группировка объектов и субъектов вокруг события;
- анализ связей лиц, объектов, событий.

RICAS — это интеллектуальная система криминального анализа данных, которая объединила в общем пространстве отображения основные и наиболее передовые методы и методики криминального анализа и аналитического поиска в реальном времени, что позволяет значительно повысить эффективность и результативность раскрытия преступлений по горячим следам и не раскрытых ранее преступлений.

Аналитическая работа в системе выполняется в автоматизированном режиме: на первом этапе по поступившему в систему запросу с помощью разработанных алгоритмов аналитического поиска автоматически осуществляется поиск, результаты которого отображаются в текстовой форме и на географической карте; на втором этапе оператором в ручном режиме осуществляется визуальный анализ полученных данных и принимается окончательное решение, либо системе задаются дополнительные, уточняющие запросы.

Система позволяет оператору выполнять многие виды криминального анализа:

- анализ криминальной обстановки (crime pattern analysis),
- анализ общего профиля (generalprofile analysis),
- анализ конкретного расследования (case analysis),
- сравнительный анализ (comparative analysis),
- анализ групповой преступности (offender group analysis),
- анализ особенностей профиля (specific profile analysis),
- анализ расследований (investigation analysis).

Используя все эти виды анализа интегрально, у оператора появляется возможность видеть картину целиком — предикативно и постфактум, т.е. систему событий, лиц, объектов, объединенных причинно-следственными связями в пространстве и времени.

Поскольку система является надстройкой над существующими базами данных, она может отображать как явно указанные связи между лицами, так и строить визуальные связи между лицами, которые, на первый взгляд, между собой не объединены. Система использует несколько алгоритмов поиска связей. Первый алгоритм — рекурсивный поиск взаимосвязей фигурантов, участвовавших в разных событиях. Второй — визуальный поиск связей. В процессе вывода специальным образом структурированной информации в визуальную среду отображения становятся очевидными связи типа «место совершения — подельник — преступник», «преступление — подозреваемый — подельники».

Инструментарий системы базируется на математических моделях и методах интеллектуального семантического анализа, визуального темпорального анализа, анализа поведенческого профиля, анализа скрытых закономерностей.

Интеллектуальный семантический анализ включает в себя мощное ядро по работе с семантикой. Анализ неструктурированных данных происходит в режиме реального времени. Для унификации поисковых функций и построения поведенческого профиля используется алгоритм классификации, или «тегирования», а также антиципационный алгоритм (схема предвосхищения), когда цель поиска известна заранее.

Семантическое ядро системы позволяет строить сложные поисковые запросы, включающие в себя всевозможные динамические и статические компоненты — ограничение по времени, методу совершения преступления, дислокации и т.д. Все функции выполняются мгновенно и позволяют максимально быстро визуализировать информацию и выполнять аналитическую работу.

Визуальный темпоральный анализ. Отображение хронологии произошедших событий и временное разграничение позволяют оперативно выявлять скрытые пространственно-временные закономерности между различными событиями.

Анализ поведенческого профиля. Наиболее постоянным и точным с точки зрения психологии преступника является его поведенческий профиль. Он отображает многие параметры деятельности преступника: привычный способ совершения преступления, места совершения и прочие мелкие зависимости, которые в совокупности соответствуют одному профилю.

Наличие тех или иных поведенческих признаков с определенной долей вероятности может свидетельствовать о том, что данный субъект может быть причастен к событию. Из этого принципа формируется так называемый групповой поведенческий анализ. Безусловно, поведенческий профиль преступника никак не может существовать без влияния на других субъектов. Поэтому в криминальной практике часто заметны совпадения по тем или иным поведенческим

параметрам у разных субъектов, когда-либо участвовавших в единых событиях. Анализ группового поведенческого профиля позволяет определять подельников, сообщников без явных связей между собой.

Анализ скрытых закономерностей. Между лицами, каким-либо образом причастными к правонарушению, объективно существуют связи (родственные, по роду профессиональной деятельности, географические — по привязке к месту жительства, по месту отбывания наказания и т.п.). Подобные связи существуют также между различными событиями. Такие связи могут быть явными, опосредованными и скрытыми. Кроме того, группа преступлений, совершенных одним и тем же лицом, обязательно имеет определенные характерные общие черты, которые явно не зафиксированы. Выявление таких скрытых закономерностей с высокой долей вероятности может идентифицировать связь между преступником и всеми совершенными им преступлениями. Безусловно, некоторые события могут выбиваться из общего потока из-за своей спонтанности или внешних факторов. Однако исходя из предыдущего принципа, такие проявления можно нивелировать.

В RICAS поиск скрытых закономерностей осуществляется, базируясь на интеллектуальном ядре обработки семантики. Семантический анализ является основополагающим, поскольку связи выражаются не всегда явно и их следует искать в контексте.

Система RICAS разрабатывалась с использованием современных оптимизированных технологий в web-пространстве и поддерживает мультиплатформность. Ее можно использовать на любых стационарных и мобильных устройствах при наличии защищенного канала связи; интерфейс системы не перегружает пользователя.

Самой известной компанией, специализирующейся на прогнозировании преступлений, является **Palantir Technologies**, вышедшая на коммерческий рынок из тени спецслужб.

Разработанные Palantir специализированные решения способны собрать воедино самую разную информацию (данные ДНК, записи систем видеонаблюдения и телефонных переговоров), отслеживать передвижения по номерным знакам арендованных машин и многое другое.

Механизм действия этого ПО заключается в анализе персональных данных и выявлении транзакций, которые всегда идут в тесной связи с паттернами, сопровождающими те или иные преступления. Иными словами, у спецслужб имеются внушительные массивы данных, среди которых сведения о финансовых сделках, отпечатки пальцев и образцы ДНК, планы зданий и топографические карты, данные радиоперехвата, «горячие» новости из СМИ, сообщения информаторов, информация из соцсетей и многое другое.

Программное обеспечение Palantir уже помогло раскрыть преступную сеть, готовящую теракты в нескольких странах мира. Его также использовали

в Афганистане для прогнозирования атак моджахедов. Кроме того, решение Palantir позволило обнаружить членов мексиканского наркокартеля, убивших сотрудника таможенной службы США. А также разрешить множество не таких громких, но не менее важных случаев, в том числе найти педофила в Нью-Йорке уже через час после нападения на ребенка, обнаружив его на видеозаписях с камер полицейского управления.

Новые технологии и большие данные нашли свое применение и в полицейских департаментах. Так, например, департамент полиции Нью-Йорка совместно с **Microsoft** разработал *Domain Awareness System (DAS) — систему, которая агрегирует и анализирует информацию об общественной безопасности из отчетов камер наблюдения, наблюдений очевидцев и т.д.* Затем эту информацию о потенциальных угрозах и криминальной активности в режиме реального времени получают следователи и аналитики департамента.

Похожим образом работает *ShotSpotter — акустическая система наблюдения*, которая фиксирует выстрелы из оружия и оповещает об этом полицию. Сенсоры ShotSpotter позволяют определить место, где произошел инцидент, с точностью до двух футов.

Но городская жизнь состоит из множества звуков, часть которых можно принять за выстрелы из оружия. Чтобы избежать таких ошибок, звуки, которые сенсоры определяют как выстрелы, отправляются экспертам. Если оказалось, что действительно произошел выстрел, то информация о том, где, когда и сколько выстрелов было совершено, отправляется полиции. Весь этот процесс — с момента, когда выстрел был засечен, до отправки информации полиции — занимает около 40 секунд. Данная технология используется уже в 75 городах США.

Система помогает не только оперативно реагировать на происшествия, но и узнавать о них, ведь жители некоторых районов часто не сообщают в полицию о преступлениях, очевидцами которых являются. Так, в городе *Милуоки* только о 14% всех выстрелов, которые зафиксировал ShotSpotter, было сообщено в полицию.

Другой частью тренда в эксплуатации новых технологий для повышения осведомленности является использование социальных медиа, и в частности Twitter. Полиция все чаще полагается на эту социальную сеть и использует ее для коммуникации с жителями города. Например, во время беспорядков, устроенных спортивными болельщиками в Ванкувере, полиция использовала Twitter для того, чтобы быть в курсе ситуации, а после того как беспорядки были устранены, Twitter и Facebook стали каналами, через которые свидетели могли сообщить полиции имеющуюся у них информацию. **Полиция Берлина** рассматривает возможность установки программного обеспечения, которое сможет предупреждать о преступлении почти как в научно-фантастическом фильме «Особое мнение», даже проект носит такое же название — Precobs. Разработанная немецкой фирмой **программа предсказывает**, где и когда с наибольшей вероятностью произойдет преступление.

Нужно сказать, что похожие программы уже несколько лет успешно работают в нескольких американских городах. Например, в 2011 г. калифорнийский город Санта-Круз (США) первым в мире внедрил математическую модель расчета вероятности преступлений, которая каждый день составляет новый маршрут для патрульных машин, основываясь на статистике преступлений по улицам. Учитываются день недели, время суток, наличие/отсутствие футбольных матчей по ТВ и другие факторы.

Патрульные полицейские Санта-Круза каждый день получают новый маршрут для патрулирования с указанием 10 «горячих точек» маршрута. Вот как выглядит эта информация в *интерфейсе Google Maps*. Для каждого квадрата размером 150 на 150 метров указывается вероятность совершения преступления в 24-часовой период, распределение этой вероятности по двум видам преступления (автомобильные и домашние), время начала двух самых опасных часовых интервалов.

Немецкая программа Pre-Crime Observation System работает примерно по такому же принципу, вычисляя вероятность совершения преступлений по тем или иным координатам, с учетом прошлой статистики.

Полиция Амстердама поставила задачу разработать программный продукт, который мог бы автоматически систематизировать тысячи полицейских отчетов, отбирая те, что имеют отношение к *торговле людьми*. Система должна была не просто отбирать подозрительные случаи, а находить закономерности, устанавливать круг людей, возможно, причастных к преступному бизнесу, то есть обнаруживать и идентифицировать потенциальных подозреваемых. В создании системы приняли участие даже российские математики из департамента анализа данных и искусственного интеллекта НИУ ВШЭ.

Главной идеей было создание хорошей системы анализа и визуализации данных полицейских отчетов. В качестве такого средства как нельзя лучше подходит анализ формальных понятий. Этот метод был предложен в 80-х гг. прошлого века немецким математиком и философом *Рудольфом Вилле*. Анализ формальных понятий позволяет визуализировать объектно-признаковые зависимости путем построения так называемых решеток формальных понятий, или решеток Галуа. Основная математическая идея заключается в возможности построения полной решетки по любому бинарному отношению и математическому описанию понятия в виде пары «объекты — признаки». В данном случае объекты — это отчеты, а признаки — информация, содержащаяся в них, например ключевые слова, даты, упоминаемые люди.

В ходе работы специалисты проанализировали порядка 70 тысяч полицейских отчетов, составленных с 2008 г. В основном это были отчеты патрульных полицейских, проводивших осмотр автотранспорта или патрулировавших улицы Амстердама. Лишь примерно в тысяче случаев полицейским было известно, что речь действительно идет о лицах, имеющих отношение к торговле людьми.

Все индикаторы (их можно выявить в тексте автоматически) разделили на группы:

- статические признаки (национальность, проблемы с документами, крупная сумма наличных, женщины не разговаривают, документы женщин находятся у водителя, проститутки, насилие, следы насилия);
- изменяющиеся признаки («район красных фонарей», дорогая машина, женщины в машине, торговля в машине, каникулы, регулярное посещение сомнительных клубов, регулярная доставка девушек в клуб);
- признаки социального окружения (человек был замечен с подозреваемым или известным преступником, сам был под подозрением).

Также индикаторы подразделялись на ранние и поздние, то есть возможные и явные, сильные признаки соответственно.

Выделенные признаки заносились в таблицу. Глядя на нее, можно было определить, сколько подозрительных признаков есть в том или ином отчете. Полицейские при составлении отчета перечислили следующие индикаторы: дорогая машина; проблемы с документами; район, где работают проститутки.

Отчет, содержащий слова-индикаторы, требовал более пристального внимания правоохранительных органов. Чтобы обнаружить и идентифицировать лиц, причастных к торговле людьми, полицейские анализируют формальные понятия.

Эта работа проходит в три этапа:

- из большого множества отчетов выделяются персоны, которые могли быть потенциально вовлечены в трафикинг;
- строится детальный профиль этих лиц, в котором отражены индикаторы и их изменение во времени;
- анализируется социальное окружение (социальная сеть) подозреваемых и эволюция этого окружения с течением времени.

Разработанный инструмент позволил полицейским в интерактивном режиме с помощью таблиц формальных понятий выделить ряд признаков и выявить потенциальных подозреваемых.

Далее с помощью разработанной системы было проанализировано и визуализировано в виде диаграммы социальное окружение человека. Программа показала, с какими людьми и при каких обстоятельствах имел дело подозреваемый. То есть, по сути, был очерчен круг лиц, возможно, причастных к ОПГ.

В деле Rolls-Royce *британское Бюро по борьбе с мошенничеством в особо крупных размерах (SFO)* впервые применило автоматизированную систему Ravn ACE, предназначенную для отбора и индексирования документов, а также извлечения из них знаний. Ранее такую работу проделывали люди, но автомат справляется с ней быстрее и не допускает свойственных человеку ошибок. С помощью ACE команда из семи человек обработала порядка 30 млн. документов, анализируя по 600 тыс. каждый день. Основная задача ACE заключалась

в сортировке документов на важные и неважные. По словам гендиректора Ravn Дэвида Ламсдена, процедура была «экспоненциально ускорена» по сравнению с ручной обработкой данных.

Между SFO и Ravn ведутся переговоры об использовании опробованной системы в других расследованиях. Одно из таких расследований было начато в августе 2016 г. в отношении подразделения гражданского авиатранспорта корпорации Airbus, сотрудники которого подозреваются в мошенничестве, подкупе и коррупции. После завершения расследования по Rolls-Royce директор SFO Дэвид Грин сообщил журналистам, что ACE умеет обучаться и пополнять свою базу знаний и за счет этого правильно отличать значимые материалы от незначимых.

Предложенная технология избавляет человека от огромного количества рутинных операций, высвобождая время для более сложной работы.

Алгоритмы глубинного поиска и индексации данных уже давно применяются аналитиками, но продукт Ravn делает еще один шаг вперед, автоматически выделяя смысл из текста, таблиц и даже изображений. Например, транснациональная компания может проиндексировать весь свой архив, все документы Word, PowerPoint, таблицы Exel и т.п. Если нужны номера паспортов 10 тыс. сотрудников, искусственный интеллект извлечет их автоматически, даже если ему предъявить только сканированные изображения паспортов.

Компания Fujitsu Laboratories Ltd. совместно с Университетом электрокоммуникаций (**Япония**) разработала алгоритм для поимки преступника в городе. Алгоритм основан на теории игр, которая математически описывает технологию защиты и нападения как технологию для принятия решений. Раньше это было сложно применить в городских условиях, так как объем информации увеличивался с размером уличной сети города. Справиться с этой проблемой позволит **технология «сжатия сети»**, разработанная *Fujitsu Laboratories Университета электрокоммуникаций*.

Разработка планов безопасности общественных сооружений (вокзалов, аэропортов) исторически основывалась на интуиции и опыте, однако в последние годы стала очевидной необходимость обеспечения повышенной безопасности с помощью искусственного интеллекта (ИИ). **Алгоритмы способны развернуть ресурсы безопасности в соответствии с движением людей и психологическими характеристиками преступников**.

Лаборатория компьютерных наук и искусственного интеллекта Массачусетского технологического института создала алгоритм, который с помощью технологии глубокого обучения позволяет ИИ использовать шаблоны человеческого взаимодействия, чтобы предсказывать, что может произойти дальше. Исследователи загружали в программу видео с примерами социальных взаимодействий людей и тестировали ее, проверяя, насколько хорошо она обучилась, чтобы быть в состоянии давать прогнозы.

Визуальные материалы для ИИ включали шестьсот часов видео с YouTube и из телевизионных сериалов. Несмотря на то что такой выбор может показаться сомнительным, одними из критериев были доступность и реализм.

Ученые представили компьютеру видео, где люди показаны за одну секунду до выполнения одного из следующих четырех действий: обниматься, целоваться, приветствовать жестами руки и пожать руку. Искусственный интеллект был в состоянии правильно угадать в 43% случаев по сравнению с людьми, которые угадывали в 71%.

Наделение ИИ умением распознавать визуальные действия, подобно тому как это делают люди, может стать предшественником разработки *интеллектуальных камер безопасности*, которые будут способны как можно раньше вызывать скорую помощь или полицию.

Это не первая попытка прогнозирования ситуации с помощью видео, но на этот раз были достигнуты более точные результаты. Причина заключается в том, что, во-первых, новый алгоритм отличается от предыдущих попыток видеопрогнозирования, в которых приоритетом была точность пиксельного представления. Он прогнозирует развитие ситуации с помощью абстрактного представления и фокусируется на важных признаках, при этом он самостоятельно обучается и использует так называемые «визуальные представления», чтобы отличать визуальные сигналы, которые играют важную роль в социальных взаимодействиях, от тех, которые такой функции не выполняют. Это вполне естественно для человека, но является сложной задачей для ИИ.

Доктор Шимей Пан из *Университета Мэриленда (США)* и работающие с ней специалисты создали в 2017 г. *нейронную сеть, которая с высокой точностью определяет, страдает ли тот или иной пользователь соцсети Facebook какой-либо зависимостью — алкогольной, табачной, наркотической*. Возможности такой диагностики система искусственного интеллекта приобрела в процессе обучения, с помощью упражнений, которые исследователи разработали на основе трех баз данных. Одна содержала 21 млн. постов, написанных 100 тыс. пользователей, участвовавших в психологических тестах. Другая — 5 млн. «лайков», оставленных 250 тыс. посетителей соцсети. Третья база включала данные на более чем 13 тыс. пользователей, о которых было известно, что они страдают той или иной зависимостью.

Итог обучения: *нейронная сеть доктора Шимей Пан выявляет наркоманов с точностью до 84%*, алкоголиков — до 81%, а курильщиков определяет правильно аж в 86 случаях из 100. И это не предел: искусственный интеллект продолжает обучаться. И когда-нибудь достигнет 100%-ной эффективности.

Японское министерство, контролирующее таможню, в 2017 г. начало полевые испытания искусственного интеллекта и дронов для борьбы с контрабандой, планируя полностью внедрить такую технологию в преддверии Олимпийских игр 2020 г.

В настоящее время таможенные инспекции в аэропортах и гаванях проводят визуальную проверку рентгеновских снимков для выявления контрабанды наркотиков и взрывчатых веществ. В дополнение к визуальным осмотрам Министерство финансов планирует использовать искусственный интеллект. С его помощью будут проанализированы уже имеющиеся в базе данных изображения, чтобы помочь выявлять контрабанду в рентгеновских изображениях.

Также будут подвергнуты анализу данные таможен о въезде и выезде людей из Японии и об экспорте/импорте грузов, чтобы определить, когда высока вероятность провоза контрабанды.

Распространение авиакомпаний-лоукостеров привело к резкому увеличению числа прибытий авиалайнеров поздней ночью и ранним утром, особенно из Азии. Новая технология может помочь ускорить проведение проверок в аэропортах, даже если ими занимаются всего несколько таможенников.

Особая активность в работах по созданию ИИ наблюдается в КНР. Первая в Китае *национальная лаборатория по разработке технологии «мозгоподобного» ИИ* открылась 13 мая 2017 г. в городе Хэфэй, являющемся административным центром провинции Аньхой (Восточный Китай). Создание этой лаборатории было утверждено Государственным комитетом по делам развития и реформ КНР. Она базируется *в Китайском научно-техническом университете* и нацелена на развитие парадигмы «мозгоподобных» вычислений и их приложений.

Данный университет известен своей лидирующей ролью в разработке технологии квантовой связи, он размещает национальную лабораторию в сотрудничестве с ведущими китайскими научными учреждениями, включая Университет Фудань и Шэньянский институт автоматизации Академии наук Китая, а также оператора крупнейшего в Китае сервиса интернет-поиска — Baidu.

Ректор Китайского научно-технического университета и председатель национальной лаборатории Вань Лицзюнь сообщил информационному агентству Синьхуа, что возможность имитировать способности человеческого мозга по сортировке информации поможет создать полную парадигму разработки технологии ИИ. Лаборатория будет проводить исследования по управлению машинным обучением, включая распознавание сообщений и использование визуальных нейросетей для решения задач.

Власти Китая с 2016 года начали вводить *систему оценки граждан по степени их благонадежности* на основе ИИ и больших данных. Каждому человеку будет присвоен некий рейтинг, от которого будет полностью зависеть его жизнь. Это касается всего — от образования до банковских кредитов.

Это не просто концепция проекта. Большая часть описанной выше идеи уже реализована и проверяется в работе властями на местах. В настоящее время в некоторых регионах страны тестируется система, которая позволяет создавать цифровые записи о гражданах. В каждой записи (анкете) будут фиксироваться детали социальной жизни гражданина и его финансовые действия.

На этой основе формируется *«рейтинг благонадежности»*, который станет определять для любого китайца возможность получения доступа к определенным сервисам, включая путешествия, образование, страхование и кредиты. Вероятно, за некоторыми категориями граждан будет установлено более пристальное наблюдение. К таким можно отнести юристов и журналистов.

В качестве примера того, как все это будет работать, можно привести обычный случай в метро. Женщина пробует пройти в подземку по студенческому билету своего сына, который стоит в два раза меньше, чем обычный билет. Ее на этом ловят полицейские и штрафуют на определенную сумму. Кроме штрафа, она получает еще и какую-то оценку, влияющую на ее общий рейтинг благонадежности. Еще несколько таких проступков — и она не сможет, например, улететь в другую страну: ей просто не продадут билет.

Конечно, потерять социальный рейтинг можно не только из-за обмана системы пропуска в метрополитене. Это касается всего — асоциального поведения, попыток обмануть налогового инспектора, нарушения правил планирования семьи.

Над системой работает как руководство страны, так и руководство более чем 30 регионов Китая.

Восемь крупных компаний Китая согласились принять участие в эксперименте правительства по разработке рейтинга граждан. В данном случае речь идет о кредитном рейтинге, который базируется в том числе на следующей информации: что и когда покупает человек, какой у него телефон. При согласии клиента могут также использоваться сведения об уровне образования и прочие данные.

Холдинг делится информацией об онлайн-покупках с государственным статистическим агентством Китая. Но персональные данные отдельных граждан не раскрываются. Это делается только в случае соответствующего запроса правительства. Причем сейчас неясно, будут ли объединены системы, собирающие открытые данные граждан страны, с теми, что ориентированы на частные данные. Скорее всего, да, поскольку еще в октябре 2016 г. Джек Ма, глава Alibaba, обратился к государственным чиновникам с призывом использовать данные из сети для выявления преступников. Правда, он не говорил напрямую о том, что Alibaba будет раскрывать данные своих клиентов и пользователей, но об этом можно догадываться. Представители компании на запрос о прояснении ситуации с заявлением Ма ответили, что речь идет о машинном обучении и глубоком анализе данных для выявления преступников.

Сейчас уже собраны **данные о кредитной истории 640 млн. китайских граждан** из 37 регионов. Еще больше данных чиновники надеются собрать из баз данных клиентов телекоммуникационных компаний Китая. Информация с телефонов, умных часов и других устройств пользователей может оказаться в этом деле крайне полезной. В целом все это похоже на северокорейский «Сонбун», только модернизированный и представленный в цифровом виде.

Тестовая работа системы позволила выявить неблагонадежных людей, преступников, которым запретили покупать билеты на самолеты и скоростные поезда. В *черный список попали 4,9 млн. человек*.

В России также используют в предупреждении преступности и терроризма новейшие технологии на основе ИИ и больших данных.

С 2007 по 2017 г. в России государственные и бизнес-структуры профинансировали 1386 научных проектов, посвященных искусственному интеллекту, на сумму около 23 млрд. рублей. Большинство проектов (1229) некоммерческие, проводятся в рамках федеральных целевых программ или оплачиваются различными фондами.

Как следует из исследования в области разработки проектов с использованием искусственного интеллекта в России, проведенного компанией SAP, *российский бизнес пока что в меньшей степени заинтересован в разработке и использовании искусственного интеллекта в своих проектах, чем государственные структуры и фонды*.

За десять лет на исследования и разработки в области искусственного интеллекта было выделено около 23 млрд. рублей. Объемы госфинансирования, хотя и выглядят впечатляюще, тем не менее сильно уступают другим странам: например, в США ежегодно из госбюджета выделяется около 200 млн. долларов на исследования в области искусственного интеллекта. Стоит также отметить, что уровень финансирования в России можно считать невысоким, учитывая количество проектов и общее число задействованных научных сотрудников (от 6 до 10 тыс. человек).

Лидеры по объему государственного финансирования — проекты для госсектора, *транспортной отрасли, обороны и безопасности*. Это свидетельствует о том, что в России прежде всего поддерживают проекты, где ожидаются результаты с быстрым применением на практике. Например, анализ данных и различные системы распознавания помогают оптимизировать логистические и транспортные проблемы. Текущие геополитические задачи также определяют острую потребность в интеллектуальных системах для модернизации оборонно-промышленного комплекса. Тематическими лидерами по вложениям со стороны государства являются проекты по анализу данных, систем поддержки принятия решений и распознавания изображений и видео (последняя тема востребована и в коммерческих проектах).

Например, основной автоматизированной информационно-поисковой системой (АИПС) ОВД на транспорте является программно-технический комплекс (ПТК) «*Розыск-Магистраль*». Этот комплекс начал внедряться в оперативно-служебную деятельность в 2000 г.

ПТК «Розыск-Магистраль» предназначен для выполнения в автоматизированном режиме следующих функций:

- выявление в пассажиропотоке лиц, находящихся в розыске, а также лиц, представляющих оперативный интерес для правоохранительных органов, посредством

автоматического сравнения баз данных по лицам, находящимся в розыске, утраченных и похищенных документов с транспортными базами данных;
- круглосуточное пополнение баз данных информацией, поступающей из ОАО «РЖД», его филиалов и структурных подразделений; предприятий авиатранспорта; ГИАЦ МВД России; информационных центров МВД, ГУВД, УВД, УВДТ; подчиненных линейных подразделений и других правоохранительных органов;
- предоставление возможности поиска по базам данных АИПС в различных режимах;
- выгрузка данных из информационных массивов АИПС и передача их в вышестоящие подразделения для формирования общероссийского (межрегионального) информационного массива;
- осуществление по запросу пользователя аналитической обработки имеющейся в базах данных ПТК информации с целью выявления и раскрытия преступлений в сфере пассажирских перевозок;
- проведение аналитических разработок по регистрируемым преступлениям и делам оперативного учета;
- формирование статистической отчетности о результатах работы системы как по выявлению лиц, находящихся в розыске и представляющих оперативный интерес, так и по количеству и качеству выданной по запросам пользователей информации.

Помимо описанных выше функций, в системе «Розыск-Магистраль» реализовано использование программных модулей — автоматизированных рабочих мест (АРМ), позволяющих выявлять и раскрывать преступления, совершенные в сфере пассажирских перевозок. В основу работы аналитических модулей заложен принцип отраслевой интеграции информации. Для каждого направления работы (по линиям уголовного розыска, борьбы с незаконным оборотом наркотиков, борьбы с организованной преступностью и др.) существует свое АРМ, позволяющее посредством специально разработанных алгоритмов извлекать из общего банка информацию и анализировать данные, необходимые для выявления и раскрытия конкретных видов преступлений.

Для информационной поддержки нарядов патрульно-постовой службы и оперативных сотрудников существуют мобильные терминалы ПТК «Розыск-Магистраль». Эти терминалы представляют собой карманные персональные компьютеры и предназначены для оперативного доступа сотрудников правоохранительных органов к информации баз данных федерального и регионального уровней, таких как «Розыск лиц», «Паспорта», «Оружие», «Угон» и др.

Мобильные терминалы позволяют:
- выявлять лиц, находящихся в федеральном или местном розыске, представляющих интерес, использующих документы, числящиеся как утраченные или похищенные;

- выявлять автотранспорт, находящийся в розыске;
- осуществлять контроль над перевозками подакцизных товаров железнодорожным транспортом.

Мобильные терминалы системы «Розыск-Магистраль» работают с ежедневно обновляющейся локальной базой данных или могут осуществлять доступ к серверу баз данных в режиме реального времени по существующему каналу связи, в том числе и с применением web-технологий.

Систему «Искусственный интеллект на границе», охраняющую российско-казахстанскую границу в пределах Челябинской области, с 2016 г. тестируют разработчики. Аналоги готовят для испытаний на Дальнем Востоке.

Разработчиком системы «Искусственный интеллект на границе» является Объединенная приборостроительная корпорация.

Пока ОПК разместила опытный комплект аппаратуры на челябинском участке границы с Казахстаном. Несколько комплектов системы готовят под установку на дальневосточных, южных участках рубежей России.

Фиксацией нарушений занимаются беспилотники, инфракрасные датчики, сейсмосенсоры, радиолокационные устройства, а передаваемая ими информация обобщается компьютерной системой с интеллектуальной программой. Наработав базу данных, программа начинает прогнозировать опасности.

Стоит задача оснастить сухопутные участки государственной границы России *интеллектуальной системой, способной автоматически собирать и анализировать информацию* о нарушении рубежей страны. Благодаря этому пограничники будут дистанционно контролировать ситуацию на границе.

На морских направлениях продолжится наращивание возможностей системы автоматизированного технического контроля за надводной обстановкой.

На сухопутных участках границы устаревшие технические средства охраны границы будут планово заменены на современные образцы. При этом стратегической целью технической политики станет последовательный переход подразделений к *дистанционному контролю за охраняемыми участками государственной границы* с одновременным сокращением использования личного состава в физической охране границ.

Речь идет о подвижных и стационарных комплексах технического наблюдения нового поколения со скрытым (практически невидимым) расположением на местности. Контролировать обстановку на удаленных и труднодоступных направлениях будут беспилотные летательные аппараты.

Кроме того, российские программисты разработали систему, которая в целях контроля над оперативной ситуацией автоматически взаимодействует с различными техническими средствами охраны: видеокамерами, инфракрасными и сейсмическими датчиками, радиолокационными станциями и беспилотниками, фиксирующими факты нарушения. Она предназначена не только для сбора различной информации, но и содержит элементы искусственного интеллекта.

Это позволяет пограничникам произвести анализ и прогнозирование ситуации, а также выработать готовые предложения по охране границ, просчитать действия и маршрут нарушителей и меры, необходимые для пресечения действий злоумышленников, с оценкой возможных рисков. При этом учитываются реальные условия местности, статистика нарушений, погодные условия, расположение пограничных постов и нарядов и многие другие факторы.

Система полностью базируется на отечественных программных решениях, которые гарантируют защиту информационных ресурсов от утечек данных, хакерских атак, других посторонних вмешательств. Данные комплексы прошли положительную апробацию в Кабардино-Балкарии, Карачаево-Черкесии, Северной Осетии и Ингушетии.

Искусственный интеллект, большие данные и квантовая криптография против киберпреступности

Аналитическое подразделение **Microsoft** по борьбе с преступлениями в сфере высоких технологий Digital Crimes Unit (DCU) было создано в ноябре 2013 г.

Важным моментом здесь остается соблюдение прозрачности схемы получения данных через **открытое государственно-частное партнерство**. У пользователей не должно оставаться сомнений относительно преследуемых целей и типов используемых сведений.

Большие данные выступают здесь в роли ультимативного инструмента расследования киберпреступлений. Внедряя очередную схему, злоумышленники повсюду оставляют цифровые следы. По отдельности эти малые изменения обычно игнорируются. Однако на уровне больших данных преступление с использованием сетевых технологий выглядит как характерный паттерн. Полностью скрыть его не удастся, как бы тщательно ни маскировались отдельные проявления.

Стало гораздо легче отследить нелегальные ключи активации программных продуктов. Раньше сами разработчики выявляли только украденные однопользовательские лицензии, когда их одновременно пытались использовать несколько человек. Сейчас обмен данными позволяет увидеть, что корпоративный ключ одной из программ украден или происходит проверка генератора ключей.

С помощью визуализации больших объемов совместных данных можно видеть необычные всплески активности на серверах регистрации, что может указывать на тестирование украденных или сгенерированных ключей. Без средств визуализации эти аномалии, скорее всего, оставались бы незамеченными.

Традиционными средствами web-мониторинга противодействовать пиратству сегодня уже вряд ли возможно. В мире существует свыше 600 млн. сайтов; с использованием больших данных выявление незаконных загрузок контрафактного ПО заметно упростилось.

Однако пиратство — далеко не единственное явление, с которым борются в DCU. Сегодня на технологиях анализа больших данных **Microsoft создает целую инфраструктуру для предотвращения любой нелегальной сетевой активности**.

Большинство сетевых атак и рассылок спама выполняются с зараженных компьютеров, формирующих ботнеты. Определение их состава и управляющих серверов — важная задача обеспечения глобальной информационной безопасности. В этом направлении работают отечественные компании, например «Доктор Веб» или «Лаборатория Касперского».

Применяя технологии анализа больших данных, в Microsoft разрабатывают алгоритмы, упрощающие определение управляющих серверов и перехват контроля над ними.

Также предупреждаются провайдеры, что компьютеры их абонентов заражены. Такое сотрудничество помогает узнать дополнительные детали о сетевой активности и вычислить дальнейшие шаги преступной группы.

Криминальные схемы постоянно меняются. Чтобы вовремя реагировать на них и отслеживать новые тенденции, сейчас важно разрабатывать универсальные аналитические инструменты, способные работать с любым набором больших данных.

Корпорация IBM объявила, что приспособила самообучающийся суперкомпьютер Watson, способный работать с информацией на естественном языке, для использования в сфере информационной безопасности.

Специалисты IBM и исследователи из восьми американских университетов планируют «скормить» самообучающейся системе содержимое библиотеки X-Force, которая содержит материалы, охватывающие два десятилетия исследований в сфере информационной безопасности, подробную информацию о восьми миллионах спамерских и фишинговых атак и описания ста с лишним тысяч уязвимостей.

На первых порах документы для Watson будут подбирать и размечать вручную, но затем машина станет справляться с этой задачей без помощи людей. На это в IBM и рассчитывают. Предполагается, что после завершения обучения, Watson будет оперативно собирать и сопоставлять общедоступные сведения о новых угрозах, в том числе информационные бюллетени, статьи, отчеты компаний, видео, даже публикации в блогах. Он будет в курсе всего, что происходит, и за счет этого сможет самостоятельно опознавать проблемы и предлагать рекомендации по их решению.

В IBM исходят из предположения, что поток информации об угрозах если еще не превысил человеческие возможности, то непременно это сделает. Национальная база данных по уязвимостям уже сейчас содержит более 75 тысяч записей и быстро растет. Каждый год публикуется порядка 10 тысяч исследовательских работ, так или иначе связанных с информационной безопасностью,

и более 60 тысяч постов в блогах по той же теме. Watson способен переварить их все. Люди — нет.

Умение Watson работать с неструктурированной информацией и сведениями, изложенными на естественном языке, сочетается с традиционными методами анализа больших данных. Система замечает аномалии, указывающие на атаки, выявляет скрытые закономерности и прослеживает связи между различными документами. Кроме того, в Watson встроены мощные средства визуализации.

Новая система борьбы с компьютерным мошенничеством на основе больших данных была разработана в **компании Visa**. В отличие от предшественников она учитывала до 500 особенностей каждой транзакции и анализировала происходящее с точностью до отдельных банкоматов. За год система останавливает мошеннические платежи на сумму примерно 2 млрд. долларов.

В том же направлении движутся и другие компании, благополучие которых зависит от эффективности системы выявления мошеннических транзакций. Кто-то, подобно Visa, модернизирует свои средства защиты самостоятельно. Кто-то внедряет или адаптирует готовые решения. Кто-то обращается к сервисным фирмам, предлагающим поиск аномалий.

Один из крупных американских банков подключил к борьбе с мошенниками суперкомпьютер Watson, разработанный в IBM (IBM умалчивает имя своего клиента, но можно предположить, что речь идет о Citigroup: об аналогичном проекте этих компаний не так давно писал журнал New Scientist). Watson известен способностью обрабатывать запросы на естественном языке, что принесло ему победу в телевикторине Jeopardy (американский прототип «Своей игры»).

Система IBM, использующая элементы Watson, анализировала поток транзакций в реальном времени, оценивая подозрительность каждой из них. На оценку, помимо прочего, влияла история отношений банка с торговой точкой, которая инициировала сделку. Чем больше мошеннических транзакций в ее послужном списке, тем меньше к ней доверия.

В IBM утверждают, что система на 15% увеличила количество выявленных мошеннических обращений к банку и на 50% сократила число ложных срабатываний. При этом сумма, которую удалось защитить от мошенников, выросла на 60%.

Те же методы работают и в других областях, причем не менее действенно. *Министерство труда Германии* приспособило их для анализа заявок на получение пособий по безработице. Скоро стало ясно, что около 20% пособий выплачивалось незаслуженно. Подобные применения Big Data в итоге позволили министерству сократить расходы на 10 млрд. евро.

Американская Комиссия по ценным бумагам и биржам (SEC) тоже автоматизировала поиск мошенников, но в данном случае речь идет не о мелких жуликах, обналичивающих краденые кредитки, и даже не о фальшивых безработных. В SEC метят выше и выводят на чистую воду мегакорпорации, совершающие финансовые нарушения.

Система выявления мошенничества, которую разрабатывают по заказу SEC, анализирует не только финансовые показатели (это самой собой разумеется), но и менее структурированные данные — вплоть до лексики, использованной в пояснениях к отчетности компании.

Компании *ZestFinance, AvantCredit и Xoom* обосновались в нишах, которые известны высоким уровнем риска, и теснят конкурентов за счет использования более совершенных технологий.

Типичный клиент AvantCredit — это человек с плохим кредитным рейтингом, попавший в трудную ситуацию. Возможно, он внезапно остался без работы. Возможно, его настигли непредвиденные медицинские расходы. Обычные банки не верят, что он сможет вернуть деньги, и отказываются с ним работать, а те, кто все же готов дать заем, компенсируют свой риск чудовищной процентной ставкой.

AvantCredit предоставляет кредиты величиной до 10 тыс. долларов и не требует гигантских процентов. *Вместо традиционного кредитного рейтинга компания использует статистические модели и алгоритмы машинного обучения, которые учитывают тысячи параметров: информацию, которую клиент предоставил сам, сведения, почерпнутые из социальных сетей, его историю транзакций и многое другое*. Чем точнее прогноз, тем меньше невыплаченных кредитов и тем выгоднее условия, которые может предложить компания.

Алгоритмы, вникающие во все детали, способны дать куда более справедливую оценку платежеспособности человека, чем банковские служащие при личной встрече.

Xoom работает в другой области, но суть та же: пока конкуренты повышают тарифы, чтобы покрыть убытки, причиняемые мошенниками, эта компания избегает убытков с помощью больших данных и предлагает клиентам более выгодные условия.

Xoom представляет собой платежный сервис для перевода наличных из Соединенных Штатов в Индию, на Филиппины, в ЮАР, а также в страны Латинской Америки и Европы. Как правило, им пользуются приезжие из стран третьего мира, чтобы отправить деньги оставшейся на родине семье.

Риск в таком бизнесе неизбежен, но алгоритмы, с помощью которых Xoom оценивает благонадежность транзакций, позволяют сократить его до минимума. Лишь 0,35% переводов приводит к убыткам. Это втрое больше, чем у платежных систем вроде Visa или Mastercard, но и задача, которая стоит перед Xoom, сложнее.

Компании, занимающиеся обеспечением кибербезопасности, всегда полагались на все более усложнявшиеся программы, которые на примере известных им вирусов обучались распознавать новые, неизвестные. К ним добавились алгоритмы, которые следят за работой других программ и оповещают об опасности, если в этой работе происходит что-то неожиданное.

Некоторые системы защиты *заключают подозрительно ведущие себя программы в виртуальный контейнер и с помощью разных методов пытаются разорвать вредоносный код и выявить его намерения.*

Появление больших объемов информации позволило сделать важный шаг на пути к созданию программ защиты, которые дают возможность перехватывать 60–70% вирусов, оставшихся незамеченными традиционным антивирусным софтом. Обучающиеся машины позволяют выявить ДНК вирусных семейств, а не просто отдельные вирусы.

Этот подход был почерпнут из мира *даталогии*, или науки о данных, и оказался очень результативным благодаря огромной базе, быстро собранной компаниями, которые начали отслеживать поведение зараженных вирусами компьютеров.

Автоматизация выявления таких аномальных шагов необходима потому, что человек или даже большая группа людей не смогут выявить их достаточно быстро.

И такие обучающиеся машины могут обеспечить защиту не только компьютерам. Когда речь заходит о крупных компаниях и даже правительствах, киберпреступники норовят проникнуть в их закрытые сети в поисках таких лакомых кусков, как базы данных клиентов, образцов новой продукции, контрактов, подробностей переговоров и ставок. Это еще одна ситуация, в которой машины заметно опережают своих создателей. Машину заставляют запомнить обширную базу данных, а затем с помощью вычислительной техники высокого уровня находить иголку в стоге сена, которой там не должно быть. Порой машина может заметить небольшую аномалию, которая укроется от человеческих глаз.

Центр по обмену и анализу информации о финансовых услугах — влиятельная организация по кибербезопасности в финансовой сфере — объявил в октябре 2016 г. о создании подразделения, целью которого является борьба с киберпреступностью и укрепление кибербезопасности финансовых институтов. Как сообщили в FS-ISAC, создание этого подразделения — результат переговоров восьми банков (Bank of America, BNY Mellon, Citigroup, Goldman Sachs, JPMorgan Chase, Morgan Stanley, State Street и Wells Fargo). Функции самого Центра по обмену и анализу информации о финансовых услугах примерно такие же, но он объединяет 7 тыс. банков. В связи с этим крупные финансовые институты решили, что им необходимо выделиться в отдельную группу, так как хакеры в первую очередь атакуют именно их, а не более мелкие банки. Новое подразделение, которое называется центром по финансовому системному анализу и устойчивости, также будет координировать деятельность банков и американского правительства в этой сфере.

В 2015 г. в структуре Банка России создан *Центр мониторинга и предупреждения компьютерных атак, осуществляемых в кредитно-финансовой сфере (FinCERT).* Основная цель создания Центра — координация работ по противодействию криминальным элементам, активность которых направлена

на личное обогащение с использованием методов несанкционированного доступа к ИТ-инфраструктуре организаций кредитно-финансовой сферы. Также организовано взаимодействие FinCERT с МВД России, ФСБ России и Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Проведенный FinCERT Банка России совместно с МВД России анализ правонарушений, выявленных в кредитно-финансовой сфере, показал, что в настоящее время основными типами правонарушений являются:

- атаки на информационные ресурсы кредитных организаций с целью вывода их финансовых активов;
- атаки на ИТ-инфраструктуру некредитных финансовых организаций — участников торгов путем использования неплатежных торговых инструментов (в том числе торговых терминалов, процессинговых сервисов).

Основными целями злоумышленников являлись как непосредственное хищение денежных средств, так и сокрытие следов ранее совершенных незаконных финансовых операций. Несмотря на то что указанные действия носят технический характер и связаны с используемыми ИТ-технологиями, они приводят к появлению значимых финансовых рисков кредитно-финансовых организаций, в том числе к нарушению обязательных нормативов к капиталу.

Банком России рассматриваются следующие основные причины появления рисков атак на организации кредитно-финансовой сферы:

- наличие множественных уязвимостей программного и аппаратного обеспечения автоматизированных систем и приложений, отсутствие должной реализации процедур контроля соответствия автоматизированных систем и приложений требованиям информационной безопасности;
- низкая эффективность мероприятий, проводимых организациями кредитно-финансовой сферы, по внедрению и использованию документов Банка России в области стандартизации обеспечения информационной безопасности;
- отсутствие правовой основы по распространению нормативных требований к обеспечению защиты информации, устанавливаемых Банком России на все процессы деятельности кредитных организаций;
- отсутствие должной достоверности контроля выполнения технических требований, как правило реализуемого в форме самооценки.

Среди ключевых направлений деятельности по снижению рисков для кредитно-финансовой сферы Банком России выделяются следующие:

- проработка вопроса о законодательном закреплении права Банка России совместно с ФСТЭК России и ФСБ России на нормативное регулирование и контроль всех вопросов, связанных с обеспечением информационной безопасности в организациях кредитно-финансовой сферы, в том числе вопросов защиты информации, отнесенной к категории банковской тайны;

- законодательное закрепление основ деятельности по реализации системы противодействия хищениям денежных средств (системы антифрод) и создание такой системы на базе FinCERT Банка России;
- обеспечение скорейшей разработки и ввода в действие национальных стандартов, регулирующих технические вопросы обеспечения информационной безопасности в организациях кредитно-финансовой сферы;
- реализация совместно с ФСБ России и ФСТЭК России системы подтверждения соответствия обеспечения информационной безопасности кредитно-финансовых организаций требованиям национальных стандартов;
- пересмотр технологических требований, связанных с осуществлением переводов денежных средств, внедрение безопасных технологий, в том числе для участников платежной системы Банка России;
- пересмотр технологии контроля со стороны Банка России за соблюдением участниками платежной системы Банка России требований к обеспечению информационной безопасности;
- реализация системы надзорных мер, учитывающей результаты контроля информационной безопасности в рамках системы подтверждения соответствия национальным стандартам.

Кроме того, ЦБ планирует создать *лабораторию, специализирующуюся на изучении технологий и последствий компьютерных атак*. Лабораторию предполагается создать в структуре самого ЦБ — на базе Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере. Прототипом такого исследовательского центра может стать уже существующий в Малайзии его аналог.

Специалисты лаборатории будут изучать способы и исходы компьютерных угроз, включая атаки на банкоматы, POS-терминалы и устройства самообслуживания. Кроме того, сотрудники ЦБ будут анализировать мошеннические интернет-ресурсы и мобильные устройства. Также новая структура будет помогать кредитно-финансовым организациям корректно снимать и опечатывать передаваемые на исследование объекты. Центробанк же со своей стороны будет готовить описание средств и методов атак на устройства самообслуживания, а также рекомендации по противодействию атакам на устройства самообслуживания.

Противоборство киберпреступников и киберполицейских идет давно: на каждый новый, более изощренный, метод защиты придумывают новые методы взлома. До сих пор борьба шла в сфере математики и кибернетики: создавались новые криптографические алгоритмы, новые методы дешифровки, новые программы для взлома, новые вирусы. Но уже близок момент, когда на поле битвы выйдет физика, и это будет *квантовая физика*.

Обычные методы шифрования имеют одно неустранимое слабое место — участникам разговора нужно обменяться ключами шифра. Пользоваться

обычной линией связи для передачи шифра нельзя: если злоумышленник эту линию прослушивает, все усилия по шифрованию будут напрасны. Поэтому наиболее важные криптографические шифры, используемые для передачи совершенно секретных государственных или военных донесений, посылают со специальными охраняемыми курьерами. Такой способ, естественно, чрезвычайно дорог. Поэтому для повседневных применений — таких как передача номера кредитной карточки с компьютера пользователя на сервер во время интернет-шопинга — используют криптографические системы с открытыми ключами, основанные на несимметричности некоторых математических операций. Так, умножить одно число на другое очень просто, но решить обратную задачу факторизации — разложения числа на множители — значительно сложнее. Например, обычному компьютеру для разложения открытого ключа длиной 2 килобита потребуется несколько сотен лет. Так, в частности, устроен широко применяемый алгоритм RSA.

Но очень скоро такие системы шифрования окажутся бесполезными: появится инструмент, способный взламывать их за несколько минут,— *квантовый компьютер*. Классический компьютер запоминает и обрабатывает информацию, записанную в двоичном коде — 0 или 1, закодированную в магнитных полях или электрических зарядах. В квантовом компьютере данные записываются в состояниях квантовых объектов — ионов, атомов, фотонов, сверхпроводящих контактах Джозефсона, которые могут находиться в суперпозиции состояний, то есть в них одновременно может быть записано сразу множество значений между 0 и 1. В момент измерения суперпозиция разрушается, квантовый бит — кубит — выдает с определенной вероятностью либо 1, либо 0. Если мы возьмем множество кубитов в определенных состояниях, заставим их взаимодействовать друг с другом, а потом считаем данные, мы можем получить решение сразу нескольких задач одновременно.

Пока настоящие квантовые компьютеры, состоящие из десятков кубитов, еще не созданы. Очень сложно удержать кубиты в определенном состоянии длительное время. Пока лучшего результата в этом добилась IBM, которая с помощью квантового компьютера из пяти кубитов смогла разложить на множители число 15. Канадская компания D-Wave выпускает квантовые компьютеры из тысячи кубитов, с которыми экспериментируют в Google и NASA. Однако машина D-Wave — не универсальный квантовый компьютер, и ее преимущество по сравнению с классическими компьютерами многими оспаривается. Российские физики пока работают только с одиночными кубитами. В частности, первый в нашей стране сверхпроводящий кубит был создан в Российском квантовом центре в 2015 г.

Даже универсальные квантовые компьютеры, когда будут созданы, подойдут не для всех вычислительных задач. Однако они имеют колоссальное преимущество перед классическими компьютерами в целом ряде применений, многие

из которых чрезвычайно важны. Универсальные квантовые компьютеры могут совершить революцию в сфере обработки больших данных, то есть в методах вычленения скрытых закономерностей и связей из больших массивов данных. Они, например, смогут оценивать закономерности потребительского поведения и предлагать товар более точно подобранной аудитории, выискивать данные о террористах в огромных массивах «цифровых» следов. Не исключено, что именно квантовые алгоритмы помогут вывести на новый уровень технологию искусственного интеллекта.

Однако поистине «взрывной» характер, предопределивший технологическую гонку в этой области, носит именно способность квантового компьютера быстро разлагать числа на множители — то есть взламывать криптографические системы с открытыми ключами. Именно она делает квантовый компьютер главным оружием в кибервойне, атомной бомбой XXI века.

Хотя до создания полноценных квантовых ЭВМ остается еще 10–20 лет, специалисты по кибербезопасности очень серьезно воспринимают эту потенциальную угрозу. Американское Агентство национальной безопасности в январе 2016 г. выпустило предупреждение и назвало криптографические алгоритмы, которые потенциально могут выдержать квантовую атаку. Однако многие из таких «постквантовых» алгоритмов неэффективны, требуя значительных вычислительных ресурсов для своей реализации, так что трудно рассчитать возможные затраты и сроки, которые потребуются на апгрейд до «постквантового» уровня в мировом масштабе. Поэтому, если квантовый компьютер внезапно окажется не в тех руках, это может привести к катастрофическим последствиям для экономики.

По странному стечению обстоятельств спасение от квантовых хакеров может принести другая квантовая технология — *квантовая криптография*. Защищенные каналы связи, которые применяются, например, для транзакций с кредитными картами, основаны на использовании ключей — кодов для зашифровывания и дешифровки сообщений. Квантовая криптография — это способ использовать законы квантовой физики, чтобы обеспечить безопасность передачи ключей. Уникальное свойство квантовой криптографии — это ее способность фиксировать любую попытку подслушать информацию при передаче.

Информация в квантовых каналах связи кодируется в квантовых состояниях фотонов — в их поляризации. Например, фотоны, поляризованные по вертикали, могут кодировать единицу, а по горизонтали — ноль. Измерить поляризацию можно только единожды, после чего его состояние необратимо меняется, а значит, если кто-то посередине линии связи попытается определить, что именно по ней передается, это сразу станет понятно получателю.

Квантовая криптография, в отличие от квантовых компьютеров, уже вполне работающая технология. Первые лабораторные устройства для защищенной квантовой связи появились еще в конце 1980-х гг., сейчас на поставках этих систем специализируются около десяти компаний. Например, компания

ID Quantigue обеспечивала защиту данных при пересылке результатов подсчета голосов на выборах в Швейцарии. По прогнозам аналитиков, объем этого рынка в 2020 г. составит 900 млн. долларов.

Препятствием для повсеместного применения квантовой криптографии является ограниченное расстояние, на которое можно пересылать фотоны. Проходя по оптическому волокну, половина фотонов теряется каждые 10–15 км, что делает передачу ключа на расстояние более 200–300 км практически невозможной.

Отчасти проблему может решить космос: Китай в этом году запустил первый «квантовый» спутник QUESS. Такой спутник проводит сеансы квантовой связи со станциями, расположенными на Земле, пока пролетает над ними. Это позволяет обмениваться защищенной информацией между любыми точками, над которыми проходит орбита спутника, как бы далеко друг от друга они ни располагались. Теоретически такой способ передачи можно взломать, однако для этого злоумышленнику придется физически захватить спутник — как, например, в фильме «Живешь только дважды» — и при этом остаться незамеченным. На практике такое вряд ли реализуемо.

Спутниковая квантовая связь, однако, недешева. Альтернативным решением проблемы расстояния может стать *квантовый повторитель* — пока гипотетическое устройство, позволяющее создавать запутанные пары фотонов, из которых можно извлечь секретный ключ. У физиков есть теоретическое понимание, как должен быть устроен квантовый повторитель, однако его практическая реализация потребует значительного улучшения технологий квантовой телепортации и квантовой памяти для света.

Еще одно препятствие — отсутствие нормативной базы, регламентирующей квантовые системы связи. Поэтому сейчас многие компании пытаются создавать гибридные устройства, совмещающие обычные телекоммуникационные стандарты с элементами квантовой защиты. Именно по этому пути идет *Российский квантовый центр*, который впервые в России запустил квантовую линию связи по обычной оптоволоконной линии между двумя отделениями Газпромбанка.

Согласно отчету ФБР «Интернет-преступность — 2017», в структуре ФБР действует несколько подразделений, связанных с борьбой с киберпреступностью. Миссия Департамента интернет-преступности (переименованного несколько лет назад в IC3) состоит в информационном обеспечении деятельности ФБР, а также во взаимодействии с бизнесом для разработки эффективных средств получения информации о киберкриминале. Эта информация анализируется и распространяется для целей оперативно- расследовательской деятельности, а также для поддержки правоохранительных органов.

История IC3

IC3 создана в мае 2000 г. как общеамериканский центр аккумуляции информации об интернет-преступности на основе обобщения данных правоохранительных

органов, бизнеса и частных граждан относительно деятельности киберпреступников, включая совершенные или задумываемые преступления.

В течение последних пяти лет IC3 получает в среднем примерно 284 тыс. сообщений в год об актах киберпреступности. Эти сообщения затрагивают не только киберпреступления на территории США, но и преступления, совершенные против американцев по всему миру.

Роль IC3 в борьбе с киберпреступностью

Каждый гражданин и юридическое лицо, зарегистрированное на территории США, имеет право подать жалобу в IC3. Информация предоставляется в соответствии с формами, разработанными Центром для каждого вида киберпреступности. В тех случаях, когда первоначальный анализ показывает, что сигнал может иметь отношение к киберпреступлению, относящемуся к компетенции ФБР, с лицом, сообщившим информацию, устанавливается оперативный контакт, и начинается повседневная работа. В других случаях информация передается по принадлежности — полиции городов, штатов и т.п.

Также Центр имеет в своем составе подразделение чрезвычайной помощи, которое в случае установления факта киберпреступления помогает жертвам принимать меры по ограничению их имущественных потерь. В рамках этой работы Центр помогает физическим и юридическим лицам установить связь с банками, кредитными организациями и т.п. для блокировки счетов и т.д.

По сути, IC3 является общенациональной базой данных о киберпреступности, формируемой не правоохранительными органами, а непосредственно потерпевшими — юридическими и физическими лицами, а также местными органами власти.

Безусловно, согласно аналитике, примерно 15–20% сообщений являются ложными, либо неточными. Однако также известно, что полиция на нижнем уровне принимает к рассмотрению и открывает дела не более чем в 30% случаев от поданных заявок, связанных с киберпреступностью. Это происходит не по злому умыслу, а из-за того, что киберпреступность имеет самый низкий уровень раскрываемости. Соответственно, полицейские не хотят «вешать» на себя нераскрытые дела. Поскольку во всех странах, за исключением США, базы по киберпреступности формируются на основе полицейских сведений, правоохранительные органы и органы власти соответствующих стран имеют перед глазами не реальную, а приукрашенную картину. Причем с каждым годом все более.

Благодаря существованию Центра IC3, оснащенного мощной программно-аппаратной инфраструктурой, компетентным профессиональным коллективом и отлаженными процедурами, правоохранители, органы власти на уровне штатов и федеральном уровне имеют наиболее точную картину киберпреступности, а граждане и бизнес — надежных помощников в трудных ситуациях.

По мере того как американские граждане получают все больше практических навыков в области информационных технологий и все больше узнают о рисках,

угрозах и преступлениях в интернете, юридические и физические лица все более точно информируют IC3, все адекватнее заполняют информационные формы и, наконец, все реже оставляют ложные или неточные сигналы о совершении применительно к ним киберпреступных действий. Если при открытии Центра доля ложных сообщений составляла примерно 35%, то в настоящее время — около 10%.

Наряду с предоставлением в ФБР или в полицейские органы на местах сообщений о преступлениях, IC3 располагает мощным аналитическим ПО, позволяющим сравнивать сообщения и объединять их в паттерны по сходным признакам. По сути, IC3 выполняет не только информационную, но и расследовательскую функцию, осуществляя на основе первичных данных распознавание по почерку отдельных киберпреступников или киберпреступных организаций, совершающих в короткое время несколько преступлений.

Поддержка правопорядка

Все американские правоохранительные органы, а не только ФБР, имеют доступ к поиску в базе данных IC3 через портал сводных правоприменений ФБР (LEEP). LEEP — это шлюз, предоставляющий правоохранительным органам, разведывательным группам и структурам уголовного правосудия доступ к уникальной базе данных IC3. База данных может быть использована, прежде всего, агентами ФБР и полицейскими на земле в любом штате США, а также следователями. Поскольку данная база доступна для всех правоохранительных органов, она позволяет осуществлять межведомственные взаимодействия правоохранителей из разных агентств и на разных уровнях. Это особенно важно для Соединенных Штатов, где множественность законодательств штатов затрудняет межведомственное взаимодействие.

Инициатива «Родник»

Инициатива «Родник» направлена на создание единой программно- аппаратной платформы для взаимодействия ФБР и других правоохранительных органов непосредственно на местах. В 2013 г., под эгидой Министерства внутренней безопасности, ФБР совместно с полицией города Солт-Лейк-Сити создало единый информационно-оперативный центр по противодействию киберпреступности на городском уровне. Если раньше в ФБР, в полиции штата Юта и в полиции Солт-Лейк-Сити были собственные программно-аппаратные центры, то с 2013 г. штат Юта покончил с этим. Теперь все правоохранители работают с единой программно-аппаратной базой, созданной ФБР. Тут собирается, обрабатывается и предоставляется информация от всех правоохранителей. Сюда также обращаются федеральные и местные агенты ФБР, сотрудники полиции штата и города в рамках соответствующей компетенции, предусмотренной законодательством. Т. е. центр один, а используется каждой правоохранительной структурой по-разному.

За четыре года отработанная в Юте структура была реализована в 13 городах США, включая Нью-Йорк, Новый Орлеан, Нашвилл, Лас-Вегас, Феникс, Лос-Анджелес и Сан-Диего. В 2018 г. система заработает в Чикаго, Питсбурге, Остине, Сан-Франциско и Сиэтле. Каждый центр указанной выше системы напрямую соединен с информационной базой IC3 и взаимодействует с ней в интерактивном режиме.

Только в 2017 г. в рамках указанного информационного сотрудничества было инициировано 27 крупномасштабных расследований, которые имели межштатный характер и потребовали подключения не только полицейских нескольких штатов, но и федеральных агентов ФБР. Обычно только на согласование компетенций уходили недели, в течение которых преступники успешно заметали следы. Фактор времени особенно важен в борьбе с киберпреступностью. Из упомянутых выше расследований 25 уже завершились арестом подозреваемых, замораживанием их активов и направлением обвинительных материалов в суды.

Главные темы борьбы с киберпреступностью

В Соединенных Штатах, согласно контенту в социальных медиа и средствах массовой информации, население страдает от изощренных хакеров и киберпреступников, взламывающих сложные корпоративные системы. Однако в реальности дело обстоит иначе. Как по «удельному весу» жалоб, так и по масштабам похищенных средств наибольшая доля приходится на мошенничества с электронной почтой.

В Соединенных Штатах в последние два года стали популярны платежные системы, синхронизированные с адресами электронной почты, а также международные платежные системы, предусматривающие взаимодействие с электронной почтой. Только в 2017 г. почтовыми мошенниками у американских компаний и частных лиц было похищено более 2 млрд. долларов. Более 70% из них приходится на мошенничества, связанные с корпоративными и частными переводами с использованием электронной почты.

В 2017 г. были взломаны системы электронной почты 19 главных исполнительных директоров компаний, входящих в список 500 крупнейших в Америке. В 13 случаях удалось установить локацию взломщиков. Это — Китай. Складывается впечатление, что китайские хакеры осуществляют киберпреступления, связанные с хищением средств, лишь для прикрытия более серьезной деятельности, направленной на хищение американской коммерческой и государственной интеллектуальной собственности. Ни одна другая страна мира не занимается в массовом масштабе такого рода деятельностью.

Новым видом преступной деятельности, связанной с электронной почтой, стал взлом электронной почты детей государственных чиновников, в том числе работающих на высокопоставленных должностях в разведывательных агентствах США. В 2016–2017 гг. было достоверно выявлено 34 таких случая. В 29 из них было четко установлено, что взлом осуществлялся с территории двух

объектов, расположенных в Китае. Эти объекты известны как инфраструктура китайской киберармии.

Впрочем, мошенничества с электронными письмами не ограничиваются шпионажем или взломом платежных систем. Ввиду широкого распространения электронной почты, осуществляются мошенничества в области лотереи, аренды, а также вымогательства. Последнее построено на нехитрой схеме. Прочтя текст, неискушенный пользователь нажимает на ссылку и тут же закачивает к себе злонамеренный блокиратор компьютера. Снятие блокировки осуществляется лишь после уплаты небольшой суммы — ориентировочно 100 долларов. Только в 2016 г. более 20 тыс. американцев сообщили о такого рода случаях в IC3.

Вымогательство

Вымогательство — это использующий вредоносное ПО вид преступной деятельности, нацеленной как на человеческие, так и на технические слабости. Основная задача — сделать доступными критически важные данные и системы. Программы-вымогатели используют не только фишинг, о чем шла речь ранее, но и поддельные сайты. В последние два-три года зафиксировано множество случаев, когда программы-вымогатели встраивались в приложения для мобильных устройств.

Если обычная программа-вымогатель нацелена на получение вознаграждения в обмен на разблокировку компьютера, то новый тип таких программ, встроенных в приложение, зачастую играют иную роль. Для ФБР уже давно не секрет, что немалая часть приложений для мобильных компьютеров создана командами и компаниями, связанными с организованной преступностью. Такого рода приложения не только выполняют свою основную функцию, но и, находясь внутри оболочки операционной системы, являются, по сути, программами-шпионами, извлекающими данные не только из мобильного устройства, но и из любых синхронизированных с ним устройств. В некоторых случаях возникает необходимость скрыть эту деятельность. Тут вступают в действие спящие до определенного сигнала программы-вымогатели. Однако они не вымогают деньги, а воспринимаются пользователями как сбой в компьютере. Соответственно, приложение предлагает обратиться в сервисный центр. Сервисный центр дает инструкцию пользователю, и, к его радости, все восстанавливается. Следовательно, у пользователя возникает большое доверие именно к этому приложению, а оно долгое время может беспрепятственно шпионить за владельцем гаджета.

ФБР жестко стоит на позиции отказа выплаты выкупа как в реальной жизни, так и в киберсреде. В этой связи Центр не оказывает какой-либо поддержки или помощи тем, кто хочет выплатить выкуп.

Высокотехнологичные мошенничества

В последние годы происходит переход от низкоуровневого к высокотехнологичному кибермошенничеству. В его основе лежит достаточно простой, но

не осмысленный обществом факт. Информационные технологии постоянно усложняются и развиваются, а в странах с высоким технологическим уровнем, прежде всего в Америке, возрастает доля технически малограмотных мигрантов первого поколения, а также людей старше 65 лет, обладающих незначительной компьютерной грамотностью. Иными словами, даже в странах — технологических лидерах постоянно растет количество людей, активно использующих интернет, но не обладающих техническими навыками. Все это ведет к тому, что производители софта стремятся максимально упростить свои программы, обеспечив доступ к интернету относительно малограмотным в этом вопросе людям.

Соответственно, киберпреступники активно этим пользуются. Мигранты и люди старшего возраста чисто психологически переносят на интернет принципы повседневной жизни. В повседневной жизни: если человек получает письмо с требованием уплатить налоги, то оплачивает их; если он видит магазин, то заходит в него и бесстрашно покупает, например, колбасу. Так же он действует и в интернете. Между тем только с 2016 г. по первую половину 2017 г. в США было выявлено больше 17 тыс. поддельных сайтов, предлагавших товары и услуги по низким ценам, казино на выгодных условиях и т.п. Точной оценки потерь пользователей от этого вида преступности не существует, но вполне очевидно, что они составляют сотни миллионов, а возможно, и миллиарды долларов в год.

В ряде штатов с высоким уровнем перехода на электронный документооборот в государственных учреждениях расцвел новый вид мошенничества. Преступники предлагают за неадекватное вознаграждение заполнить за жертву (лицо с низкой компьютерной грамотностью) те или иные документы в рамках предоставления страховки, пенсии, миграционных документов и т.п. Помимо немедленного вознаграждения, они оказываются обладателями номеров социального страхования, платежных реквизитов и т.п. Вопреки ожиданиям, количество такого рода преступлений в технологически развитых Соединенных Штатах не падает, а из года в год увеличивается. Только в 2017 г. IC3 зарегистрировал почти 17 тыс. подобных случаев. Установлено, что прямой ущерб составил незначительную сумму — 15 млн. долларов. Однако косвенный ущерб подсчитать невозможно, поскольку в руках у преступников оказалось около 1 тыс. критически важных сведений о человеке.

Нелегальная миграция и интернет-преступность

Из года в год, начиная с 2005 г., устойчиво растут объемы и разнообразие киберпреступных действий в отношении нелегальных мигрантов. По состоянию на 1 января 2018 г. в Америке насчитывается не менее 12 млн. нелегальных мигрантов. Это составляет чуть менее 4% населения страны и по численности соответствует населению Португалии или Гондураса, Коста-Рики и Гватемалы, вместе взятых.

Как показывают данные миграционной службы и полицейских подразделений на местах, нелегальные мигранты быстро осваиваются с американскими

реалиями и стремятся как можно быстрее воспользоваться многочисленными благами. Они так же, как американские граждане, хотят приобретать товары и услуги на Amazon, выполнять разовые работы на Uber, осуществлять сделки на eBay и т.п. В то же время они боятся предоставлять адрес своего места жительства для доставки товаров или пользоваться кредитными картами, через которые миграционная служба может выйти на них.

Таким образом, в последние три-четыре года в Америке сложилось два сектора киберкриминала, связанных с обслуживанием нелегальных мигрантов. Один сектор интернет-преступности сопряжен с оказанием услуг по введению в заблуждение миграционных и правоохранительных органов. Частично в общедоступной Сети, частично в сети TOR анонимно можно приобрести номера социального страхования, некоторые из которых являются не поддельными, а украденными у американских граждан, постоянно проживающих за рубежами США.

Таким же образом обстоит дело с кредитными картами и автомобильными правами, в некоторых штатах по-прежнему заменяющими удостоверения личности. По данным ФБР, в течение 2015–2017 гг. было продано минимум 1,2–1,5 млн. подобных поддельных документов по цене от 200 до 1000 долларов. Парадокс этой процветающей отрасли состоит в том, что по законодательству миграционная служба не занимается интернет-преступностью вообще. Полициям штатов заниматься ей затруднительно, поскольку подобные криминальные торговые площадки идентификационными документами имеют общеамериканский характер и зачастую зарегистрированы в Канаде или Мексике как местах платежа. Что же касается ФБР, то при предыдущей администрации организация особо не занималась пресечением рынков нелегальных документов для нелегальных мигрантов.

Второй сектор интернет-преступности, связанный с нелегальной миграцией, носит посреднический характер. Как известно, американские интернет-ритейлеры, и прежде всего Amazon, традиционно не доставляют товары в целый ряд стран, включая Россию, Китай и т.п. Соответственно, в течение последних пяти-шести лет сложился посреднический сектор. Посредники предоставляют на прокат американские адреса, а иногда и платежные реквизиты для взаимодействия с ритейлерами, которые отгружают товары именно на эти адреса, а затем посредник обеспечивает их доставку в те страны, с которыми по тем или иным причинам Amazon или иная компания не работает напрямую. Это — законная деятельность, полностью соответствующая законодательству. Поэтому правоохранительные органы не преследуют подобных посредников.

Однако в условиях роста благосостояния нелегальных мигрантов, который произошел из-за высокого уровня их нелегальной занятости, у мигрантов появились деньги для покупок. Так сформировался слой посредников, которые для внутренних американских нелегальных покупателей оказывают те же

услуги, что легальные посредники — для внешних. Отличить нелегальных от легальных посредников в интернете весьма сложно. Более того все нелегальные посредники с удовольствием оказывают и легальные услуги.

Состояние дел с основными видами интернет-преступности

Вымогательство

В американском уголовном правосудии под вымогательством понимается требование преступника от жертвы заплатить за какие-либо действия, связанные с восстановлением данных, или за соблюдение режима конфиденциальности в отношении персональных данных, разглашение которых может повредить жертве. В последние годы термин «вымогательство» стал широко применяться и к интернет-преступлениям. В части интернет-преступлений вымогательство сводится к трем основным видам преступности:

- блокировка компьютеров и гаджетов и разблокирование в обмен на выплату определенной суммы;
- похищение или шифрование важных для пользователя файлов с их возвращением и дешифрованием в обмен на платеж преступнику;
- угроза раскрытия информации, полученной преступным путем, которая может навредить частной, общественной либо деловой репутации пользователя.

С 2015 г. все чаще жертвами вымогательства становятся дети и пожилые американцы. Вымогательство у детей связано, как правило, не с принуждением их к денежному платежу, а с сокрытием той или иной конфиденциальной информации о них в обмен на эротические или сексуальные съемки и фотографии детей, используемые затем в качестве контента для педофилов.

Что касается пожилых американцев, то в 2016–2017 гг. была пресечена деятельность крупной русскоязычной банды, рассылавшей электронные письма пожилым людям, у которых внуки или правнуки обучаются и проживают в других, удаленных от местожительства данных пожилых людей, местах. В письмах сообщалось, что внуки попали в неприятную ситуацию и урегулировать ее можно только в том случае, если пожилые люди переведут средства на счета преступников.

В последние годы для платежей вымогатели все чаще используют виртуальные валюты, прежде всего Bitcoin и Monero.

В 2017 г. в Соединенных Штатах было зафиксировано более 32 тыс. случаев вымогательств. Только в трети из них преступники были найдены и понесли наказание. Наибольшее распространение вымогательство получило в следующих штатах: Калифорния, Техас, Колорадо, Флорида, Пенсильвания, Южная Вирджиния, Нью-Йорк и Огайо. Наиболее низкий уровень преступности, связанной с вымогательством, имеет место в Вашингтоне, Орегоне, Миссисипи и Луизиане. Во всех этих штатах в течение 2017 г. количество вымогательств не превысило 100 случаев.

Определение типов преступлений

В 2017 г. американские правоохранители, включая ФБР и полицейские силы, стали работать с новой классификацией:

1. Платежное мошенничество. Это распространенный в Соединенных Штатах вид преступности, когда преступные группы (в основном африканские и азиатские) рассылают письма, в которых предлагают корреспондентам значительные суммы денег. В качестве условия выплаты этих денег предполагается осуществление предварительных платежей, как правило, связанных с оплатой юридических и прочих услуг для осуществления платежа. Если в 90-е и нулевые годы основным источником подобных писем была Африка (и они даже получили название «нигерийские письма счастья»), то в последние годы письма приходят из Венесуэлы, Перу, Эквадора и Боливии.

2. Предварительный взнос. Все чаще преступники посылают электронные письма, в которых указывают, что получатель квалифицирован финансовой компанией на получение льготного крупного кредита или выиграл значительную финансовую премию. При этом, по условиям кредита или премии, предполагается, что получатель предварительно должен оплатить некрупные (обычно до 500 долларов) расходы, связанные с юридическими пошлинами за оформление сделки. Жертва платит авансовый взнос и никогда больше не получает новых писем.

3. Социальная инженерия как подкрепление электронного мошенничества. Этот тип мошенничества используется против юридических лиц, имеющих обширный круг контрагентов. Сначала пользователь получает письмо, где при помощи традиционной техники ссылок заражается компьютер. Такого рода письма в основном отправляются автоматизированными корпоративными системами безопасности в корзину. Через три-четыре часа после направления письма раздается телефонный звонок и звонящий интересуется, получено ли письмо и передано ли оно руководству. После такого звонка, согласно обследованиям, примерно в 60% случаев секретари разыскивают письмо, жмут на ссылку и запускают троян в корпоративную систему.

4. Благотворительность как преступление. Преступники все чаще создают ложные благотворительные организации. Обычно это происходит после серьезных стихийных бедствий. После этого они на хорошо оформленных бланках направляют письма со ссылкой на реально действующий сайт и просят сделать небольшие пожертвования. Американцы, как правило, сопереживают в таких случаях, и больше половины обращений оказываются действенными. Люди делают пожертвования, будучи абсолютно уверенными, что они отправляют деньги законным благотворительным организациям.

5. Мошенничество на доверии. В последние годы в Соединенных Штатах все шире стало распространяться мошенничество на доверии. Если раньше это происходило только через электронную почту, то с середины нулевых годов все

активнее используются социальные сети. В этом случае создаются поддельные профили реальных людей, которые по тем или иным причинам не представлены в интернете. После трех-шести месяцев поддержания профиля в актуальном состоянии — с постами, «лайками» и т.д.— квазиличности выступают с предложениями организовать вечер выпускников колледжа или игроков футбольной команды университета, которая играла 20 лет назад, и т.п. В основной своей массе американцы — доверчивые люди и с удовольствием участвуют в разного рода коллективных мероприятиях ностальгического характера. Поэтому они поддерживают подобные инициативы и в ответ на предложение заранее снять ресторан, отель и т.п. выражают согласие, переводя деньги. Только в 2017 г. было зарегистрировано более 3 тыс. мошенничеств на доверии, в результате которых преступники похитили более 200 млн. долларов.

6. Утечка корпоративных данных. В большинстве случаев хакеры добывают корпоративные данные с помощью методов социального инжиниринга. Также значительная часть информации утекает вместе с покидающими компанию сотрудниками. Примерно в 30% случаев кража корпоративной информации, по данным соответствующего подразделения ФБР, осуществлялась исключительно с использованием программных средств. Примерно в 40% случаев — с комбинированным использованием социального инжиниринга и программных средств. Еще в 30% случаев у интернет-преступников были сообщники внутри компании.

7. Карточное мошенничество. Среди всех видов интернет-преступности, нацеленной на население, наибольший ущерб в 2016–2017 гг. причинило карточное интернет-мошенничество. Общие потери населения США от этого вида мошенничества за два года составили более 1,1 млрд. долларов. Выделяются три основных типа интернет-мошенничеств с кредитными картами.

Первый — это так называемые поддельные платежные хабы. В интернете размещаются сайты с распродажами по очень низким ценам тех или иных вещей, товаров и т.д. Гражданам предлагается разместить на сайте платежные реквизиты, включая фамилию, номер карты, идентификационный код и т.п. В случае если то или иное физическое лицо попадает в число тех, кому хватило ограниченной партии товара, с него сразу будет снята указанная на сайте сумма. Хитрость мошенничества, запущенного только в 2017 г., в том, что незначительное число граждан действительно получают престижные качественные товары со скидками до 90%. При этом преступники получают сотни, а часто и тысячи необходимых платежных реквизитов. Эти реквизиты передаются специалистам по взломам, и те уже работают с банками, для того чтобы снять средства.

Второй тип интернет-мошенничества с платежными картами достаточно традиционен. Он описан был ранее: это услуги по предоставлению краденых платежных карт нелегальным мигрантам.

Третий тип мошенничеств с кредитными картами является наиболее эффективным. На него приходится до 80% от общей суммы похищенных средств.

В настоящее время в Соединенных Штатах лишь у 25% владельцев компьютеров и менее чем у 12% владельцев гаджетов стоят мощные платные антивирусы, включающие в свой состав утилиту безопасных платежей. У остальных — бесплатные антивирусные программы, не предохраняющие от перехвата платежной информации и присвоения преступниками средств с банковского счета.

8. Интернет-преступность против детей. К данному виду интернет-преступности относятся любые виды киберпреступности, объектом которых являются дети. В Соединенных Штатах выделяются три вида интернет-преступности против детей: интернет-вымогательство; незаконное включение встроенных в компьютеры и гаджеты видеокамер; принуждение детей к съемкам контента для педофильского сообщества.

Наиболее важные статистические факты об интернет-преступности

К концу 2017 г. общий ущерб, нанесенный киберпреступниками и интернет-вымогателями домохозяйствам, бизнесу и органам власти всех уровней, превысил 5 млрд. долларов за год. По сравнению с 2015 г. сумма денег, полученных преступниками, по данным ФБР, увеличилась в непредставимые 15 раз. В 2017 г., по данным Министерства внутренней безопасности, 90% полученных киберпреступниками в результате вымогательства сумм, переводились с использованием криптовалют. Порядка 90% от нанесенного ущерба пришлось на юридические лица, и лишь 10% — на домохозяйства. Среди юридических лиц первенствовал средний бизнес. На него пришлось более 60% вымогательств.

Очевидно, что интернет-преступники, обладающие достаточно высоким технологическим уровнем, не хотят тратить время на домохозяйства из-за невысокого размера возможной добычи и боятся проводить преступные операции против крупного бизнеса, ИТ-компаний и финансового сектора, располагающих мощными внутренними службами информационной безопасности. Поскольку в Соединенных Штатах более 60% ВВП производится малым и средним бизнесом, эти предприятия сочетают относительную информационную беззащитность с хорошим финансовым положением. Поэтому именно они становятся жертвами кибервымогателей в первую очередь.

Согласно статистическим данным Министерства внутренней безопасности и бизнеса, по-прежнему самой большой проблемой для частного сектора остается фишинговая почта, используемая интернет-преступниками. По данным ФБР и Министерства внутренней безопасности, в 2017 г. более 30% среднего американского бизнеса подверглось хотя бы одной кибератаке. Это лишь те случаи, о которых бизнес сообщил правоохранительным органам. Есть основания полагать, что реальное количество как минимум в два раза выше.

Согласно отчету Verizon's 2017 Breach Investigations, 92% вредоносных программ по-прежнему доставляются по электронной почте. 56% руководителей компаний среднего американского бизнеса сообщили, что почти в 2/3 случаев

фишинговые атаки были успешны и преступникам удалось проникнуть во внутренние корпоративные сети, используя доверчивость, недостаточную осведомленность персонала в азах компьютерной безопасности.

Если раньше для того, чтобы злоумышленники могли проникнуть в системы корпоративной безопасности, персонал должен был нажать на ссылку, то теперь используются более изощренные способы. Во-первых, к письму прилагаются безупречные по внешнему виду pdf-файлы с проектами договоров, информацией о компании-отправителе, товарах и т.п. При скачивании файла параллельно загружается невидимый троян, встроенный в проект договора,— он и становится шпионом в корпоративной сети. Во-вторых, ныне электронные письма используют для того, чтобы активировать шпионские программы, уже стоящие на компьютерах и оказавшиеся там из-за синхронизации личных гаджетов сотрудников с корпоративной сетью (это происходит в основном на малых и средних предприятиях).

Подавляющее большинство американцев полагают, что интернет- преступники в первую очередь выбирают банковские учреждения. Однако это не так. По данным Министерства внутренней безопасности, уже третий год подряд наиболее уязвимым для интернет-преступников является американское здравоохранение. Происходит это по ряду причин. С одной стороны, здравоохранение испытывает недостаток как в кадрах, так и в программно-аппаратных средствах безопасности. Многие, особенно штаты Великих Равнин, разрешили сотрудникам использовать в медучреждениях для служебных целей собственные компьютеры и гаджеты. Они, как правило, имеют устаревшие операционные системы и интернет-браузеры и буквально напичканы шпионским и вредоносным софтом. С другой стороны, медицинские учреждения являются кладезем информации для интернет- преступников. Часть этой информации (в первую очередь, платежные реквизиты и медицинские записи) они используют для кражи денег, а также для шантажа и вымогательства. Другие — продают.

Сегодня ФБР оценивает подпольный рынок медицинских данных в сумму, превышающую 3 млрд. долларов. Покупателями медицинских данных являются не только преступники, но и — через посредников — легальный бизнес, фармацевтические компании, пенсионные фонды, строительные подрядчики, специализирующиеся на медицинском секторе.

Наконец, начиная с 2017 г., дополнительный спрос как на похищенные данные, так и на уязвимости в информационных системах медицинских учреждений, стали проявлять крупные преступные синдикаты, а также банды киберкиллеров, осуществляющих убийства с использованием интернета вещей.

Крайне настораживающим фактором стало усиливающееся из года в год сотрудничество низкоуровневого интернет-криминала с обычными, в целом законопослушными американскими гражданами. Согласно данным Business Insider, в 2017 г. в среднем 60% сотрудников при уходе с работы по собственному

желанию или увольнении забирают с собой конфиденциальные данные компании, в том числе (практически во всех случаях) пароли от корпоративной сети компании. В darknet существуют процветающие рынки покупки паролей. В некоторых случаях цены доходят до 50 тыс. долларов.

В последние пять лет Департамент внутренней безопасности по соглашению с Институтом Гэллапа проводит обследования в части киберпреступности. Если в 2012 г. только 52% американцев беспокоились, что хакеры похищают их личную информацию, то в настоящее время — 67%. В 2012 г. примерно 40% топменеджеров компаний беспокоились о состоянии информационной безопасности. В настоящее время таковых 66%.

Наибольший уровень беспокойства у американцев вызывают кражи информации по кредитным картам, а также налоговая и финансовая информация. Об этом волнуются 69% американцев. Наименьшее беспокойство американцы проявляют к возможности угрозы со стороны интернет-преступности в отношении детей — 18%, использованию похищенных данных для убийства через интернет вещей — 5%, краже данных о месте проживания и т.п.— 2%.

Классические методы защиты сетей работают недостаточно эффективно: вызовы, с которыми сталкиваются специалисты, требуют новых механизмов и инструментов борьбы с атаками, которые бы соответствовали уровню развития технологий. Даже современный файрвол с IPS неспособен качественно противостоять уязвимостям нулевого дня (таким как WannaCry). Традиционная защита на уровне терминалов тоже не обеспечивает должный уровень безопасности от подобного рода угроз, поскольку системы, как правило, не успевают за потоком новых угроз и работают в экстренном режиме. Даже в комплексном сочетании они часто не дают необходимого эффекта из-за сложности интеграции решений разных производителей и трудностей в предотвращении горизонтального распространения угроз.

В качестве ответа на новые вызовы в области информационной безопасности китайская компания *Huawei* предлагает решение для обнаружения и нейтрализации угроз Huawei SDSec. Это *трехуровневая система активной сетевой защиты на основе искусственного интеллекта*: на первом уровне проводится анализ с использованием алгоритмов искусственного интеллекта и обработки больших данных, который отправляет на карантин весь подозрительный сетевой контент и неизвестные вредоносные файлы. На втором уровне разворачиваются центр управления безопасностью и центр управления сетью, разработанные Huawei для различных сценариев: они могут централизованно управлять политиками безопасности во всей сети, организовывать службы безопасности и быстро развертывать их на базе пользовательских сервисов и приложений в течение нескольких минут. Третий уровень — это непосредственно ИТ-инфраструктура: коммутаторы, маршрутизаторы, межсетевые экраны, сервера и системы хранения, беспроводные сети, на которых и реализуются политики управления сетью

и безопасности. Такой подход к обеспечению сетевой защиты должен значительно сократить среднее время обнаружения угрозы и восстановления инфраструктуры, а общие затраты на управление и поддержание ИТ в адекватном состоянии, по данным вендора, можно снизить на 80%.

Традиционные методы обеспечения информационной безопасности часто не справляются с новыми угрозами. Для обеспечения безопасности сегодня все чаще используют инновационные подходы к построению систем защиты с применением технологий больших данных и искусственного интеллекта. Такие системы глубоко интегрированы в ИТ-инфраструктуру предприятия, и в частности в сетевую среду. Huawei разработала решение, построенное по новым принципам активной сетевой защиты, которая позволяет проактивно реагировать на информационные угрозы и предотвращать потенциальные проблемы с безопасностью.

Борьба с биткоин-преступностью и использование технологии блокчейн для предупреждения преступности

В 2016 г. Европол, Интерпол и Базельский институт управления договорились о создании *совместной рабочей группы, специализирующейся на цифровых валютах.*

В задачу группы входит сбор и анализ информации о преступном использовании цифровых валют, расследование вопроса о хранении доходов, полученных преступным путем, организация ежегодных семинаров и встреч представителей трех ведомств и других учреждений, а также создание сети специалистов по биткоин-преступности.

Одновременно *нью-йоркский стартап Chainalysis* и Европейский центр Европола по борьбе с киберпреступлениями подписали соглашение о сотрудничестве и обмене данными, чтобы противостоять онлайн-преступлениям.

Меморандум о взаимопонимании между блокчейн-компанией и Европолом должен способствовать поиску и наказанию биткоин-вымогателей.

Chainalysis специализируется на идентификации злоумышленников, отслеживая их действия в блоковой цепи. Команда разработчиков стартапа работает над программой, которая будет соблюдать конфиденциальность клиентов и в то же время предотвращать взлом системы.

В 2015 г. была сформирована государственно-частная инициатива «Блокчейн-альянс» с целью борьбы с преступной деятельностью в области блокчейна и биткоина.

«Блокчейн-альянс» — это некоммерческая организация, которая была создана *Палатой цифровой коммерции и организацией Coin Center.* В состав Альянса входят «*Инициатива цифровой валюты» Медиалаборатории МТИ*, разработчик Гэвин Андресен, *компания BitFinex* и некоторые другие компании и организации.

Все они объединились для того, чтобы рассеять опасения касательно преступного использования криптовалюты биткоин и технологии блокчейн.

Standard Chartered Pic и DBS Group Holdings Ltd. собираются создать блокчейн-реестр инвойсов, чтобы сократить издержки и предотвратить мошенничество, с которым сталкиваются компании, финансирующие международную торговлю.

Соображения конфиденциальности мешают банкам обмениваться информацией о совершаемых ими транзакциях, что позволяет недобросовестным клиентам использовать одни и те же документы многократно. Именно поэтому *технология блокчейн, гарантирующая прозрачность всех транзакций, могла бы стать решением проблемы инвойс-мошенничества*.

Блокчейн позволит перенести в цифровую среду то, что даже в эпоху интернета остается на бумаге. До сих пор мы боимся потерять страховые полисы, выписки о недвижимости из Росреестра; компании выпускают бумажные акции; избиратели на выборах опускают в урны бумажные бюллетени. Все эти документы имеют аналоги в информационных системах, но необходимость многоуровневых проверок не позволяет исчезнуть их офлайн-двойникам.

Блокчейн — цепочка блоков, в которую можно вписать любую информацию без изменения предыдущих записей,— может помочь оцифровать любую информацию в мире, а доступ к ней — без рисков и ущерба — сможет иметь любой желающий. Блокчейн выступает этаким «эликсиром доверия»: благодаря архитектуре сети (невозможность редактирования изменений, уже внесенные в базу данных, без согласия большинства участников) провайдер инфраструктуры, который раньше выступал гарантом доверия, теряет свою исключительную роль.

Блокчейн можно сравнить с учетной книгой. Из нее нельзя тайком вырвать страницу, в ней нельзя подрисовать нолик к уже записанному числу — записи книги хранятся в виде копий и распределены среди разных людей в тысячах экземпляров (точно так, как цепочки блоков в сети блокчейн хранятся на множестве узлов). Поэтому блокчейн можно использовать в любых сферах, где децентрализованные реестры позволят проводить операции с цифровыми активами безопаснее и эффективнее.

В конце 2015 г. DBS и Standard Chartered протестировали распределенную платформу TradeSafe, на которой планируют запускать инвойс-реестр. Кроме того, они активно сотрудничают с сингапурским ведомством, ответственным за развитие инновационных технологий.

Но внедрение блокчейна снимет проблему мошенничества только в том случае, если перейти на распределенную цепь решится сразу большинство банков.

В мире нет единых стандартов в регулировании цифровых валют, и каждый центральный банк руководствуется собственными подходами: от формального разрешения (включая рекомендации для индустрии по поводу возможных рисков, исследования в данной области и пр.) или применения общих принципов регулирования в сфере платежей до полного запрета такой деятельности. Если рассмотреть, какие могут быть последствия в условиях формального

разрешения осуществлять деятельность с цифровыми валютами, то центральным банкам, придерживающимся такого подхода, следует обратить внимание на негативную статистику банкротств цифровых бирж (в том числе связанных с мошенничеством и хакерскими атаками). Решением данных проблем могло бы стать, например, *лицензирование деятельности, связанной с виртуальными валютами*, деятельностью бирж виртуальных валют, или администрированием и эмиссией виртуальных валют, или хранением и управлением третьих лиц.

Многие специалисты полагают, что осуществление полного запрета на указанную деятельность в условиях общемирового регуляторного тренда на формальное разрешение такой деятельности в рамках специальных лицензий *может привести к свертыванию инновационных проектов в данной сфере* и перенесению их в более прозрачную регуляторную юрисдикцию.

Автор первой книги про биткоины *Алекс Форк* полагает, что блокчейн может использоваться в рамках национальной платежной системы. Создается отдельный, независимый блокчейн для национальной платежной системы; граждане попадают в блокчейн, когда получают «персональный счет», привязанный к паспорту. Любой участник может пользоваться переводами в этой системе — без комиссии. Законодательно закрепляется, что одна единица в этом блокчейне равна, например, рублю. А все деньги (любое количество) первоначально эмитируются на одном «**персональном счете**» (например, ЦБ РФ).

«Персональный счет» — это цифровой документ на предъявителя. Он представляет собой набор букв и цифр. Его можно смело передавать другой стороне без раскрытия личности. Только государственные органы могут верифицировать пользователя по счету. Для этой платежной системы могут быть применимы различные интерфейсы: приложение на ПК, web-версия (оплата через личный кабинет), оплата с помощью мобильных устройств, в том числе NFC, QR-code, оплата с помощью платежных карт.

Преимуществами такой платежной системы являются: 100%-ная прозрачность движения средств в стране; скорость движения денег (практически мгновенно — до 2 секунд); подтверждение за 10 минут; надежная защита безопасности; контроль за движением бюджетных средств и простота управления ими (может быть осуществлено силами одного человека); исключена возможность отмывания денег; блокчейн также предусматривает дополнительные возможности (автоматическое налогообложение физических и юридических лиц, применение на разных платформах: мобильное приложение и т.д.).

Национальные банки Белоруссии, Казахстана, Великобритании, Молдовы внимательно изучают возможности блокчейна.

При этом необходимо отличать саму технологию от конкретных криптовалют. Технологии распределенной обработки, включая bloclchain и bitshares, действительно изучаются как на уровне регуляторов, так и на уровне коммерческих организаций. В Банке России создана рабочая группа, которая изучает

вопросы технологий распределенной обработки и учета финансовой информации. Ее цель — проанализировать основные тенденции и практики в этой области, а также определить подходы к регулированию.

Борьба с преступностью и 3D-принтеры

Еще в начале XXI века сотрудники правоохранительных органов обратили внимание на то, что доступность подробных 3D-моделей ДТП или мест преступления приводит к существенному повышению оперативности и результативности работы следственных органов. Вместо измерений, производимых современными криминалистами с помощью архаичной рулетки, достаточно будет пары щелчков мышки. Преимущества 3D-фото особенно очевидны для баллистической экспертизы и анализа объемных отпечатков подошв и протекторов, а также для каталогизации 3D-фотопортретов подозреваемых, поскольку традиционные снимки в профиль и анфас ограничивают точность опознания преступников, которые могут быть запечатлены охранными системами наблюдения в самых произвольных ракурсах. Кроме того, 3D-фото могут повысить эффективность идентификации подозреваемых по форме ушных раковин и иным подобным индивидуальным чертам.

Несколько производителей 3D-сканеров с начала века внедряют их технологии в деятельность ФБР. По мере развития технологии 3D-печати, возможность быстрого и доступного производства реальных физических объектов из компьютерных моделей распространяется во все сферы жизни. И сегодня 3D-печать действительно может быть использована для раскрытия преступлений.

Главный департамент полиции Токио теперь использует 3D-принтер для **воссоздания 3D-модели места преступления**. Напечатанные 3D-модели помогают следователю и прокурору лучше объяснить события преступлений. Вместо того чтобы показывать присяжным фотографии с места преступления, прокурор может продемонстрировать подробную 3D-модель с планом этажей и расстановки мебели.

3D-принтер был представлен *Институтом научных исследований при Департаменте полиции Токио* в 2010 г. Он был использован для поиска доказательств по делам — например, черепа жертвы в делах об убийстве. В *Университете штата Алабама в Бирмингеме* 3D-принтер был использован для воссоздания отпечатков ног.

Модели следов в настоящее время создают из гипса, по технологии парижского литья, при помощи фотографий с места преступления. Но разработка системы, которая может сканировать отпечатки ног и рук в 3D, имеет ряд преимуществ.

Если у вас есть следы в виде цифровых изображений, вы можете легко сравнить их друг с другом, чтобы создать более объективную картину, нежели вы могли бы, опираясь на результаты анализа человеком. Поскольку можно напечатать модель, которая не требует обработки, в отличие от гипсового слепка, вы создадите несколько абсолютно идентичных копий.

С одной стороны, подделать папиллярный узор пальцев сможет любой владелец 3D-принтера. Использование отпечатков пальцев для доступа к банковским счетам — только малая область того, где может происходить **идентификация человека по уникальному папиллярному узору**. Профессор *Мичиганского университета* Анил Джейн почти всю свою жизнь работает в сфере биометрических технологий, разрабатывая системы распознавания человека по отпечаткам пальцев и радужной оболочке глаз. Как известно, они уникальны для каждого человека, как и ДНК-код. Профессор Джейн плотно сотрудничает с компаниями, которые разрабатывают биометрические системы доступа. Например, совместно с ZKAccess ученый создал технологию идентификации пациентов для детской больницы.

В 2016 г. к А. Джейну обратилась полиция штата Мичиган с необычной просьбой. Требовалось содействие расследованию, а именно создание **отпечатка пальца мертвого человека**. Нужно было сделать протез пальцев мертвого мужчины, чтобы снять блокировку с мобильного телефона, который был защищен доступом только при помощи удачного распознавания отпечатка пальца владельца устройства. Следователи считали, что разблокированный мобильник жертвы мог бы помочь найти убийцу, ведь на телефоне могла остаться какая-нибудь фото- или аудиоинформация, которая повела бы полицию по следам преступника. Работники полиции посмотрели выложенный на YouTube ролик с участием профессора Джейна, в котором показывалось, как можно отсканировать отпечатки пальцев человека, а потом с их помощью создать поддельные искусственные пальцы и обойти защиту сенсоров мобильных телефонов.

Сотрудники полиции штата дали команде Анила сканы отпечатков пальцев жертвы, которые были сделаны задолго до нападения. В процессе работы над этим делом профессор Джейн вместе со своим студентом воспроизвел копии пальцев человека. Первым делом они преобразовали двухмерные отпечатки пальцев в трехмерные. Сделано это было при помощи 3D-принтера: пальцы распечатывались по аддативной технологии — слой за слоем, при этом в качестве материала использовался мягкий пластик. Он обеспечивает сохранение мельчайших неровностей верхнего слоя кожи, что и дает почти идеальное совпадение искусственного отпечатка пальца с оригиналом.

Когда копия пальца владельца смартфона была готова, на ее поверхность были нанесены тончайшие слои серебра, золота и меди. Это потребовалось для воспроизводства электропроводности, подобно живой коже человека. Если не наносить слои металла, а просто использовать пластиковую копию пальца, телефон, защищенный сенсорным доступом, разблокировать невозможно — пластиковый материал не обладает необходимой электропроводимостью. После создания пластиковой копии пальца ее сразу же передали сотрудникам полиции для продолжения расследования.

Перед созданием пальца жертвы при помощи 3D-принтера команда эксперта биометрии Анила Джейна пробовала воспроизводить собственные отпечатки пальцев на том же принтере, с применением той же технологии. С помощью напечатанных пластиковых пальцев ученые сняли блокировку со своих телефонов той же марки, что и у жертвы расследуемого преступления.

Джош Веинбергер, бывший студент юридического колледжа Университета Стетсона, в 2015 г. начал новый проект под названием 3D Printed Evidence. Он сотрудничает с провайдером услуг 3D-печати и 3D-сканирования — компанией Forge.

Компания занимается *изготовлением точных копий и масштабированных моделей, связанных с доказательствами по преступлениям*. В настоящее время вещественные доказательства используются в залах судебных заседаний, чтобы справедливо и точно представить реальные объекты, которые имеют значение в деле, например снимки костей потерпевшего или даже всего места преступления. Следователи и ученые используют гипс для создания слепков следов или масштабные копии отпечатков пальцев с цветовой кодировкой ребер. Картонные модели, компьютерные анимации и другие виды моделей уже являются обычной практикой.

Процесс создания печатных 3D-моделей доказательств довольно прост, ведь все модели от начала до конца создаются специалистами самой компании. На месте преступления следователи могут использовать передовое фотограмметрическое программное обеспечение, такое как PhotoModeler Scanner или 3DReality, для создания точных копий отдельных предметов или моделей всего места преступления. Цифровые модели также можно изготовить по фотографиям, сделанным на цифровую фотокамеру. Затем модели подготавливаются к печати и печатаются.

В будущем эту технологию смогут применять сами представители правоохранительных органов, для этого им нужно будет просто воспользоваться портативным 3D-сканером.

В настоящее время модели стоят 200–400 долларов — вполне доступная цена, учитывая стоимость создания компьютерных анимаций и прочих форм доказательств.

Полицейская служба в Австралии с помощью портативного 3D-сканера может с высокой точностью зафиксировать **компьютерные модели внутренних и наружных сцен преступления**. Сканер «Зеведей» ранее использовался для создания моделей известных достопримечательностей и кораблекрушений, однако теперь эта технология может быть применена для борьбы с преступностью.

Преимущества этого прибора заключаются в том, что он сводит к минимуму нарушение сцены происшествия, экономит время и предоставляет возможность добраться до ранее труднодоступных мест типа уничтоженных следов или осмотреть кустарников.

Тщательное исследование мест совершения преступлений на открытом воздухе (в том числе в густых лесах, пещерах и других обширных территориях)

обычно занимает множество времени. С помощью «Зеведея», также известного как ZEB1, теперь полиция может с легкостью получать доступ к таким местам и ограниченному пространству, где иногда бывает сложно установить громоздкое оборудование для камер и штативов. При вращении прибор испускает лазерные лучи и непрерывно сканирует окружающую среду. Он способен делать более 40 тыс. кадров в секунду. В отличие от колесных мобильных систем «Зеведей» может собирать данные на лестницах и на пересеченной местности, а также в районах, где нет GPS.

Используя данные, собранные с помощью сканера, следователи полиции могут быстро воссоздать сцену происшествия на компьютере в формате 3D, а затем найти и отметить маркером улики, определить интересующие их участки и даже повернуть комнату или пейзаж для просмотра под любым углом. Эту технологию разработали сотрудники Государственного объединения научных и прикладных исследований в Брисбене в 2010 г. Ранее «Зеведей» использовали для съемки объектов Всемирного наследия в попытке сохранить их.

Программисты из *Университета Корнелла (США)* **научили нейросеть создавать точную 3D-модель лица человека по одной фотографии**. Программа уже создала 3D-изображения Мохаммеда Али, Иэна Кертиса и Дональда Трампа. Для обучения нейросети авторы использовали снимки из Chicago Face Database, содержащей сотни фотографий людей разных рас и возрастов. Сначала программа распознает по фотографии форму лица и создает для него карту альбедо, определяющую диффузный цвет, который виден при освещении предмета белым светом. После этого сверхточная нейросеть VGG-19 анализирует изображение, распознает отдельные части лица и подбирает к ним реалистичные текстуры. Недостающие детали изображения система реконструирует самостоятельно, сравнивая модель с другими изображениями из базы. Система также может убирать лишние шумы, если исходное изображение плохого качества. Разработчики считают, что эта программа пригодится для создания собственных трехмерных аватаров, *для реконструкции внешности погибших и пропавших людей*.

Как пишет Science, группа ученых из *Имперского колледжа Лондона* разработала в 2017 г. алгоритм, который позволяет наиболее точно воспроизводить 3D-модели человеческих лиц. Новый метод предназначен для поиска преступников, проведения пластических операций и создания масок в Snapchat.

Наиболее распространенная сейчас модель для создания 3D-лиц (3DMM) обычно имеет в базах данных ограниченный набор типов внешности — в основном взрослых белокожих людей. Из-за этого точность создания модели лица весьма невысока.

Новый метод, созданный группой ученых во главе с Джеймсом Бутом, позволяет автоматизировать создание 3D-моделей. Алгоритм сканирует фотографию, сразу же выделяет основные черты лица (например, кончик носа), потом

выравнивает сканы по ориентирам, если нужно, ищет совпадения в библиотеке лиц. Свой алгоритм группа Бута проверила на основе 10 тыс. сканов лиц, сделанных пластическими хирургами Алланом Понниахом и Дэвидом Данвэем в Музее науки Лондона. Так, они загрузили фото ребенка в новый алгоритм и обычный 3DMM. Первый смог создать правдоподобную 3D-модель, второй выдал вместо этого 3D-версию головы взрослого человека.

Как правило, сейчас при создании компьютерных моделей лиц используется метод трехмерной морфологической модели (3D Morphable Model, или 3DMM). В качестве «основы» берется нечто вроде каркаса, который представляет собой набор параметров, характеризующих величину отклонения ключевых точек. Каждый параметр нужно настраивать вручную, а затем еще и доводить до ума итоговую модель в 3D-редакторе. Английские ученые же разработали метод полной автоматизации процесса составления 3DMM-моделей, что позволяет включить в них данные, полученные от достаточно большого количества людей. Этот алгоритм автоматически выстраивает снимки лица одного человека согласно их пространственной ориентации и составляет на базе них трехмерную модель. Кроме того, при помощи все того же алгоритма можно выявить ошибки и удалить их из конечных результатов.

В процессе разработки компьютерная система проанализировала огромное количество изображений лиц людей различных национальностей, возраста и пола. В результате обработки данных была составлена модель среднего человеческого лица, названная Large Scale Facial Model (LSFM). Новая LSFM-модель была использована для генерации 100 тыс. изображений, примененных при обучении системы искусственного интеллекта на базе нейронной сети. Затем нейронная сеть научилась самостоятельно преобразовывать двухмерные снимки лиц людей в достаточно точные трехмерные модели.

Сейчас исследователи заняты усовершенствованием алгоритма с целью обучения системы распознаванию человеческих эмоций, что значительно улучшит и без того широкие возможности нового способа 3D-моделирования.

Постепенно исчезают различия между изображениями реальных и созданных компьютером ненастоящих людей. Люди настолько хорошо способны распознавать других людей, что чрезвычайно трудно создать искусственный объект, который выглядит как нормальный и здоровый человек. Сейчас научились очень хорошо делать такие компьютерные изображения человека, на которых он выглядит почти как реальный, но большой проблемой остается сделать так, чтобы он имел вид нормального человека.

Японские художники Теруюки и Юка Ишикава начали в 2015 г. свой проект по созданию с помощью компьютера очень реалистичного образа выдуманной школьницы. Ее зовут Сая, и с тех пор она стала выглядеть значительно лучше.

С помощью аналогичных технологий можно создавать *анимацию подозреваемого преступника*.

Можно сказать, фантастических результатов, необходимых для расследования преступлений, достигла *студентка Хизер Дюи-Хагборг,* **создав 3D-портреты из ДНК, найденных на сигаретных окурках и жевательных резинках на улице**.

Последовательности ДНК она вводит в компьютерную программу, которая создает облик человека с образца. Обычно в ходе этого процесса выдается 25-летняя версия человека. Затем модель распечатывают в 3D-портрете в натуральную величину.

Важно для борьбы с терроризмом: научные достижения, позволяющие видеть сквозь стены и читать по губам

1. **ОРРИ (обратно-рассеянное рентгеновское излучение)** — технология, при которой рентгеновские лучи от источника не проходят сквозь объект, а отражаются. Так как объект не надо просвечивать насквозь, возможно использовать излучение с интенсивностью на несколько порядков ниже, чем при проникающем.

К числу веществ с малой атомной массой относятся взрывчатые и наркотические вещества, алкоголесодержащие жидкости, ткани тела человека. Это дает возможность легко идентифицировать скрытые органические материалы или людей, которые могут представлять угрозу безопасности.

Использование технологии ОРРИ позволяет:

- получать изображения органических предметов, плохо различаемых при обычно используемой технологии проникающего рентгеновского изучения;
- размещать источник и приемники излучения в устройствах досмотра, расположенных с одной стороны от досматриваемого объекта;
- создавать за счет малой мощности излучения устройств, использующих данную технологию, системы, которые безопасны для операторов и людей.

2. **Переносной радар «Голограф»** (испытания в частях российского спецназа начались в 2014 г.), обнаруживающий людей и животных через стены, в течение следующего года поступит на испытания в спецподразделения Вооруженных сил. Разработка *Центрального научно-исследовательского института химии и механики* предназначается для использования в контртеррористических операциях и должна помочь быстро скоординировать действия отряда и обезопасить заложников. Доработка устройства возможна после испытаний радара военными.

Это устройство в первую очередь необходимо подразделениям антитеррора, которые работают с учетом сохранения жизни заложников.

Другое назначение — когда есть какие-то материалы или объекты, которые нельзя повредить. Например, борт самолета, где придется работать врукопашную, перед этим разобрав себе цели, посмотрев, кто где находится и где возможно неожиданно обрушиться на врага,— это 50% успеха. Радар мог бы спасти очень много жизней.

Радар «Голограф» работает при помощи сверхкоротких радиоимпульсов на частоте от 1 до 4 ГГц, пропуская их через любые материалы и принимая отраженный

сигнал, и обнаруживает движение на расстоянии до 6,5 м. Устройство обладает небольшими габаритами и весом 4,5 кг, выдерживает падение на бетон с высоты 1 м и может использоваться при температурах от –20 °С до +50 °С.

Любой человек, даже новобранец, сможет пользоваться устройством через 15 минут после того, как ему объяснят принцип работы. В нем очень мало настроек (их практически нет), есть кнопка включения и очень доступная индикация.

«Голограф» способен распознавать движения сквозь кирпич, бетон, дерево, гипс, глину, сухой грунт и штукатурку. Как рассказал представитель разработчика, в каждом отдельном случае у радара разные возможности, но главное — чтобы материал не содержал воды.

Все зависит от материала стены: сквозь дерево он «видит» на метр; если это кирпич — то полметра; а бетон уже должен быть тоньше, потому что там есть железо. Кроме того, еще очень важно, насколько материал стены влажен: если это свежепостроенное здание и кирпич или пеноблоки не высохли, то видно хуже — волны гасятся, мешает вода.

Помимо сырого кирпича, проблемой может стать совместное использование «Голографа» с устройствами, заглушающими сигналы сотовой связи. Данная возможность ограниченно испытана: при низкой мощности излучателей радар не реагирует на мобильные телефоны, Wi-Fi-роутеры.

3. **Ученые научились видеть людей через стены с помощью Wi-Fi**

Компания Technische Universitat Ilmenau (ФРГ) создала в 2017 г. уникальный высокочувствительный компактный прибор, который позволяет с высокой степенью детализации смотреть сквозь препятствия. Разработчики устройства утверждают, что оно дает возможность заглянуть за бетонные и кирпичные стены даже многометровой толщины. Специалисты компании убеждены, что их «всевидящее око» поможет в полицейских и спасательных операциях, а также в борьбе с терроризмом.

Однако новость о создании «всевидящего» девайса не вызвала особого восторга у людей. Многие опасаются, что прибор немецкой компании может быть использован не только правоохранителями и спасателями, но и террористами, ворами, коммерческими агентами, сотрудниками политического надзора, извращенцами, «озабоченными» вуайеристами и просто неадекватными людьми.

Представители компании, конечно же, уверяют, что будут контролировать распространение «всевидящих» приборов, которые могут использовать не по назначению.

Издание USA Today сообщило, что практически все американские спецслужбы для обнаружения людей внутри зданий применяют радары RANGE-R. Это, по мнению авторов статьи, вызывает опасения относительно масштабов государственного надзора в США.

Стоимость одного RANGE-R равна 6 тыс. долларов. В описании прибора говорится, что «запатентованная L-3-технология ступенчатой частоты непрерывной

волны (SFCW) и собственные алгоритмы обнаружения цели позволяют радару работать, как высокочувствительный детектор движения Доплера», но американцы продают RANGE-R как типовые авторадары.

Другие «всевидящие» устройства, такие как трехмерные дисплеи, имеют куда более продвинутые возможности. Пентагон уже широко использует подобные приборы в военных целях в Афганистане и Ираке. Также проекты по разработке систем, отображающих интерьеры зданий, спонсирует и Министерство юстиции, которое якобы планирует применять их для налоговых целей.

Пока такие устройства остаются дорогостоящими и для использования требуют особых навыков, но наука не стоит на месте. *Совсем скоро заглянуть за стены любого дома можно будет и с помощью обычного Wi-Fi.*

Физики Массачусетского технологического института (МТИ) придумали в 2016 г., как с помощью обычного Wi-Fi-передатчика можно видеть людей сквозь стены. Причем не просто видеть, но и даже определять вес и рост человека. Ученые уверены, что новая технология понадобится спецслужбам и правоохранительным органам.

Физики из МТИ несколько преобразовали работу обычного Wi-Fi-маршрутизатора и научили его в буквальном смысле «видеть» объекты, находящиеся в соседней комнате. Технология работает довольно просто: маршрутизатор передает через стену Wi-Fi-сигналы, которые отражаются от предметов и возвращаются назад, отображая картинку на экране компьютера. Затем ученые «натаскали» модифицированные передатчики на распознавание человеческих силуэтов, а дальнейшее улучшение алгоритма привело к тому, что маршрутизаторы научились определять точный рост и вес человека.

Такая технология по большому счету уже достаточно давно известна, но, как признали ученые из Массачусетса, она была рудиментарной.

Вопреки этому мнению, 23-летний студент из Мюнхенского технического университета Филипп Холл совсем недавно доказал, что Wi-Fi уже достиг возможностей, позволяющих получать *качественные голограммы или трехмерные фотографии объектов* из другой комнате, используя всего два небольших устройства. Ему потребовалось всего 20 секунд, чтобы сосканировать в достаточно качественную объемную картинку все то, что было у него за стенкой. «Можно различить фигуру человека или собаку на кушетке»,— пояснил разработчик.— «Любой предмет размером более 4 сантиметров».

Чтобы «смотреть» сквозь стену, Холл использовал лишь две крохотные антенны вроде тех, которыми оснащены обычные смартфоны. Полученная антенками информация была обработана специальной программой, которая отображала ее в виде качественной 3D-голограммы.

В принципе, сквозь тонкие преграды позволяет «видеть» и *обыкновенный прибор ночного видения*, действующий на основе *приема и распознавания инфракрасного излучения*. Известны также и просвечивающие сканеры, которые

используют в аэропортах для поиска спрятанных под одеждой предметов. Но, скажем, для условий боевых действий нужно что-нибудь более «зрячее», способное на большом расстоянии распознавать противника, спрятавшегося не за фанерной ширмой или тканевым пологом, а за кирпичными стенами, панельными плитами и т.п.

Перспективно выглядит разработка ученых *Мэрилендского университета (США).* Они сканируют пространство за преградой при помощи радиоволн в терагерцевом диапазоне (31011–31012 Гц) — так называемых Т-лучей.

Приборы, использующие излучение такой частоты, уже применяются в медицине наряду с рентгеновскими аппаратами. Т-лучи совершенно безвредны для биологических объектов. Но сложность их использования заключается в том, что до сих пор это было возможно только при температурах, близких к абсолютному нулю.

Вторая проблема — визуализация изображения, полученного отраженным от объекта Т-лучом. В медицине эта задача решалась при помощи графеновых пластин — модификации углерода с повышенной подвижностью электронов в кристаллической решетке. Благодаря этому свойству Т-луч получает возможность «нагреть» и «выбить» эти электроны из графеновой пластины. Вследствие чего на пластине возникает положительный потенциал, который и помогает зарегистрировать и визуализировать исследуемый объект.

Но как американским ученым удалось довести столь сложное оборудование до размеров, при которых его можно использовать в реальной боевой обстановке? Или же был испытан всего лишь лабораторный образец, демонстрирующий принципиальную пригодность метода?

Симферопольская компания «ЭМИИА» разработала технологию, позволяющую «видеть» движение людей, животных, жидкостей, а также различных объектов сквозь стены.

Новый прибор использует эффект Доплера — изменение частоты и длины волн, регистрируемых приемником, вызванное движением их источника и/или движением приемника. В текущем виде система объединяет два компьютера и специальные сканирующие устройства.

В зависимости от типа и материала преграды система позволяет «смотреть» сквозь стены и другие оптически непрозрачные препятствия в радиусе до 50 м. В настоящее время изобретатели переносят свое детище на мобильную платформу и разрабатывают микрочип, который можно будет внедрять в различные аппараты и носимые гаджеты.

«В перспективе устройство может выглядеть как планшетный компьютер или шлем для бойца. Оно может устанавливаться на беспилотные летательные аппараты и передавать информацию на землю. Эта технология сможет заменить аварийные датчики и охранные устройства»,— сообщают в компании «ЭМИИА».

В Росгвардии апробированы уникальные *портативные радары, способные «видеть» людей даже через толстые стены*. Изделие позволит спецназовцам вычислять террористов не только в зданиях, но и в замаскированных блиндажах и подземных тоннелях.

Новейший *радар-стеновизор РО-900, разработанный группой компаний «Логис-Геотех»*, способен определять местонахождение движущегося человека на расстоянии до 21 м, при этом он «видит» сквозь несколько кирпичных или бетонных стен общей толщиной до 60 см. Это позволит бойцам Росгвардии с безопасного расстояния обнаружить террористов не только внутри зданий, но и на самой дальней их стороне, определить траекторию перемещения, а боевиков, стоящих неподвижно, радар обнаружит по дыханию. При этом сам стеновизор очень компактен, его вес не превышает килограмма.

Стеновизор РО-900 уже прошел все испытания, подтвердил характеристики и в настоящее время поставляется одной из российских спецслужб. К изделиям также проявляют интерес МВД и другие силовые ведомства. Особую заинтересованность выразили представители МЧС, которые планируют использовать радар для поиска людей в завалах.

Стеновизор РО-900 работает по принципу георадара-локатора, который способен проводить радиоволны не только по воздуху, но и через грунт и стены зданий и регистрировать все отражения от препятствий.

РО-900 похож на обыкновенную рацию без антенны. Он оснащен 3,5-дюймовым цветным дисплеем, который в реальном времени отображает результаты радиолокационной разведки. Полученные данные выводятся на экран в виде движущихся по диагонали красных полос (вертикальное направление экрана отображает информацию о расстоянии, на которое переместился человек, а горизонталь позволяет определить время, за которое был совершен маневр).

Радар также регистрирует повторяющиеся движения с небольшой амплитудой, засекая таким образом расширение грудной клетки во время вдоха или биение сердца. Уже после 20 секунд анализа полученных данных радар выводит информацию об обнаружении затаившегося человека на дисплей в виде горизонтальной синей черты.

Эксперты считают, что стеновизор станет огромным подспорьем в боях или контртеррористических операциях в городе.

Чтение по губам

Исследователи из Оксфордского университета при поддержке DeepMind и NVIDIA разработали машинный алгоритм чтения по губам LipNet, который распознает текст с точностью до 93%.

В отличие от существующих алгоритмов чтения по губам, LipNet распознает не слова по отдельности, а фразы и предложения целиком. Как показали испытания программы на базе данных GRID, ее точность достигает 93,4%. По

данным разработчиков, это на 40% превышает средний результат людей с нарушениями слуха, которые используют чтение по губам в повседневной жизни как метод коммуникации (52,3% точности).

Машинное чтение по губам имеет огромный потенциал для использования в борьбе с преступностью: распознавание речи в шумной обстановке, биометрическая идентификация и реставрация аудиозаписей.

Технологии чтения мыслей преступников

Уже сейчас компьютерные программы позволяют читать мысли и даже отображать их на экране. Журналист Татьяна Громова еще в 2014 г. удачно обобщила возможности новых технологий.

Так, исследователи из Калифорнийского университета в Беркли работают над созданием **декодера, способного считывать мысли человека, а также отображать их в видеоформате**. Когда человек читает газету или книгу, он слышит звучащий в голове внутренний голос. Такая виртуальная речь является следствием мозговой деятельности, и, если расшифровать возникающие в ходе этого процесса образы, можно выяснить, о чем думает человек.

Во всяком случае, как вариант создания нового типа детектора это — весьма перспективное направление.

Возглавивший исследование Брайан Пэсли поясняет, что, когда человек слышит речь, акустические колебания воздуха возбуждают сенсорные нейроны в его внутреннем ухе. Сигналы от этих нейронов передаются в мозг, который путем сложной обработки интерпретирует звуки в слова. Именно на стадии обработки звуковых сигналов в мозге сконцентрировала внимание группа Брайана Пэсли.

В своих исследованиях ученые работают с пациентами, которым для борьбы с эпилепсией уже были внедрены электроды в определенные участки мозга. Записи сигналов мозговой деятельности, снятых при помощи электродов, показали, что в мозге присутствуют группы нейронов, реагирующих на звуки с различными характеристиками: к примеру, одна группа возбуждалась при звуке частотой в 1000 Герц, другая — в 2000 Герц. На базе этой информации составили компьютерную программу, которая может распознать звуки и расшифровать слова, услышанные испытуемыми. Позже ученые выяснили, что алгоритм, способный считать то, что слышит человек, может «читать» и его мысли.

Видео мыслей. Чуть позже команда Брайана Пэсли научилась создавать видео мыслей человека. Данная технология работает по тем же принципам, что и чтение картины мозговой деятельности. Установка **функционального магнитно-резонансного сканирования** считывает образы, которые появляются в мозгу у человека, когда он смотрит видео, а затем проводит корреляцию этих образов с изображением на экране. На основе таких данных создана **компьютерная модель, которая соотносит картины мозговой деятельности с изображениями**.

Для этого ученые накопили огромную базу данных, включившую 18 млн. секунд видеороликов, взятых на YouTube, и образы мозговых волн, соответствующих этим видеороликам.

Алгоритмы программного обеспечения выбирали наиболее близкие по содержанию видеоролики уже через одну-две секунды после начала анализа мозговой деятельности. Затем мысленные образы и выбранные видеофрагменты объединялись, демонстрируя картину мыслей.

Технологию будут использовать для разработки устройств, получающих видеоизображение прямо из мозга людей. Они, в частности, помогут пациентам, которые не могут говорить в силу различных причин физиологического или психологического характера (например, потерпевшие, пережившие сильный стресс при насилии).

Увеличение разрешающей способности датчиков и более совершенные алгоритмы программной обработки сигналов позволят также создавать портативные устройства, которые найдут применение в самых разных сферах. Так, дизайнер сможет сразу увидеть на экране воплощение своих идей. Такие аппараты смогут служить и для записи сновидений, воспоминаний, а также проведения исследований в области психологии и психиатрии.

Специалисты из *нидерландского Университета Неймегена* создали программу, позволяющую воспроизводить то, что читает человек без произношения текста вслух. Возглавивший проект Марсель ван Джервен рассказывает, что интересующую часть головного мозга условно разбили на участки (объемные пикселы) размером 2×2×2 мм, и вся дальнейшая математическая обработка оперировала значениями среднего уровня активности нервных тканей каждого из участков. Выполняя ряд сложных преобразований, удалось восстановить изображения рассматриваемых объектов, а также нечеткие, но вполне узнаваемые изображения символов текста.

После этого ученые ввели в математическую модель данные о том, как на самом деле выглядят символы текста. Это значительно улучшило способность программы его распознавать: она сравнивает получаемые данные с начертаниями каждого символа и выбирает тот, который наиболее точно подходит к считанному из мозга образу. В результате получается содержание, максимально приближенное к реальному.

Со временем *ученые намереваются использовать технологию для воспроизведения того, что человек видел и читал ранее, также его сны и фантазии.* Достичь этого позволит мощный сканер MRI, который способен предоставить данные с более высокой точностью и разрешающей способностью. Это дает возможность оперировать большим количеством объемных пикселов (15 тыс. против 1,2 тыс. нынешних).

Спецслужбы и правоохранительные органы разных стран мира давно используют *программы, которые по движениям губ, челюстей и мышц лица*

человека могут распознать слова, которые произносит человек. Но интонации и эмоциональная составляющая таким программам были не по силам.

Используя высокоскоростную камеру, делающую тысячи кадров в секунду, *исследователям из Университета Васеда в Токио* удалось сделать запись даже мельчайших колебаний поверхности кожи лица и шеи человека, которыми сопровождаются звуки, исходящие от голосовых связок. После съемки специализированная компьютерная программа, основанная на сложнейших алгоритмах, превратила снятые колебания кожи в голос человека. При этом сохранилось не только содержание, но и все интонации, определяющие эмоциональную окраску речи.

По словам руководителя научной группы Ясухиро Оикоа, камера снимала с частотой 10 тыс. кадров в секунду. Для сравнения: в обычном видео используется съемка с частотой 24 кадра в секунду, а особо качественное видео снимается с частотой 60–80 кадров в секунду. Голоса добровольцев записывались с помощью обычного микрофона, а колебания кожи их лица и горла регистрировались с помощью датчиков-виброметров.

Компьютерная программа выдала рассчитанную на основе визуальных данных последовательность звуковых колебаний, которые затем сравнили с реальными, записанными с помощью микрофона и виброметров. Выяснилось, что компьютерные данные почти полностью совпадали с действительностью. Проигрывая получившийся звуковой файл, исследовали смогли достаточно четко **распознать отдельные фразы и голосовые интонации**. Технология в первую очередь будет использоваться правоохранительными органами при расследовании обстоятельств преступлений.

В 2017 г. ученые из японского Технологического университета в Тоёхаси разработали устройство, по последним имеющимся данным электроэнцефалограммы (ЭЭГ), *определяющее односложные слова и отдельные цифры, о которых размышляет человек*.

Изобретение японцев в качестве базы использует механизм работы электроэнцефалограмм, которые сканируют мозговые волны, возникающие, когда человек что-то произносит. Потом эти волны соотносятся со слогами и цифрами с помощью «машинного» обучения, применяемого для разработок искусственного интеллекта.

В процессе исследований при помощи аппарата удалось с точностью до 90% отгадывать цифры от 0 до 9, о которых думал человек. Ученые отмечают, что до этого проблемы появлялись именно в процессе декодирования электроэнцефалограмм.

Они даже предположили, что такое управляемое мобильным приложением устройство будет массово выпускаться уже в 20-х гг. этого столетия.

В 2017 г. революционный прорыв в чтении чужих мыслей начала осуществлять сеть **Facebook** во главе с ее основателем **Марком Цукербергом**.

Известно, что у Facebook в 2016 г. появилось секретное подразделение с ни о чем не говорящим названием *Building 8*. Род занятий новой структуры журналисты смогли определить по объявлению о наборе сотрудников. За сложной формулировкой скрывалось чтение и отображение мыслей без физического вмешательства в работу мозга. Марк Цукерберг анонсировал технологию, благодаря которой пользователи социальной сети смогут читать мысли своих друзей. О том, что в Facebook начали разработку технологии, благодаря которой пользователи соцсети в будущем смогут неким образом «слышать» мысли, которые будут думать их друзья, заявил основатель и владелец компании Марк Цукерберг: «Я думаю, однажды мы сможем посылать друг другу мысли с помощью технологий. Компания Facebook занимается разработкой технологии, которая в будущем позволит читать мысли…»

Напомним, еще в 2015 г. создатель Facebook Марк Цукерберг заявил, что люди смогут делиться своими мыслями напрямую на основе исключительно технологий. Мечта Марка Цукерберга — создать такой **гаджет, который позволит людям читать мысли друг друга**.

Facebook действительно может создать гаджет, напрямую связанный с мозгом владельца, считает российский психофизиолог *Александр Каплан* (см. «Росбалт» от 21.01.2017).

Скорее всего, по его мнению, речь идет о создании смартфона нового поколения с элементами технологии нейроинтерфейсов. Эта технология позволяет человеку научиться изменять электрическую активность своего мозга — правда, в небольших пределах. Изменения регистрируются, расшифровываются электроникой и уже цифровым кодом передаются к приемникам внешних исполнительных устройств, например, для управления компьютерной клавиатурой. Со стороны это выглядит как мысленное управление компьютерной клавиатурой: человек смотрит на экран — и там буква за буквой появляется текст. Понятно, что это далеко не чтение мыслей, но действительно реальное управление напрямую от мозга. Элементами технологии можно оснастить и смартфон.

К настоящему времени более 200 научных лабораторий довели нейроинтерфейсы до очень высокого уровня эффективности. Пользовательским структурам типа Facebook или Google остается только внедрить разработки ученых в конкретные продукты. Специалисты Facebook умеют это лучше, чем ученые в научно-исследовательских лабораториях. Понадобится лишь плотное взаимодействие между ними. Цукерберг заключил контракты с 14 университетами, чтобы поддерживать такого рода проекты.

Смартфоны научатся не «читать мысли», а по реакциям ЭЭГ распознавать, какую из 20–30 команд задумал в данный момент пользователь. И это действительно будет некоторый прорыв, потому что до настоящего времени смартфоны управлялись нажатием кнопок или голосом. Теперь они станут понимать безмолвные команды. И скорее всего, такая революция будет связана не столько

с телефонными звонками, сколько с работой в социальных сетях. Насколько известно, Facebook собирается создать специальные графические интерфейсы, для того чтобы с помощью новых смартфонов входить в соцсеть и оперировать там ее объектами. То есть в сетях появятся специальные настройки, которыми будет достаточно легко управлять усилием мысли.

Уже сейчас Интернет достиг той стадии развития, при которой приближенные к искусственному интеллекту алгоритмы, работающие, например, на серверах социальной сети Facebook, могут «чувствовать» эмоциональное состояние пользователей. К таким выводам пришли ученые из Австралии, которые проводили специализированные эксперименты в «Фейсбуке» (2017 г.).

Гнев, радость, а также иные эмоциональные состояния — все это учитывается алгоритмами социальной сети. Соцсеть умеет определять эмоциональную окраску слов, используемых в сообщениях.

Глобальные навигационные системы в борьбе с преступностью

В 2015 г. в Волгоградской академии МВД России Нина Юрьевна Дусева защитила весьма интересную диссертацию на тему: «*Технико- криминалистические основы использования глобальной навигационной системы в расследовании и предупреждении преступлений*».

Место и время совершения преступления как элементы события преступления подлежат установлению по каждому уголовному делу независимо от того, имеют они значение для уголовно-правовой квалификации содеянного или нет. Источниками такого рода информации являются в числе прочих информационные системы, функционирующие в различных областях гражданского сектора и имеющие разное целевое назначение.

Интеграция разрозненных данных, хранящихся в массивах перечисленных подсистем, **в единую глобальную навигационную систему**, а также разработка программно-технического комплекса для работы с данной информацией позволят накапливать, хранить и осуществлять аналитическую обработку пространственно-временных данных о различных объектах, представляющих интерес для правоохранительных органов, а также обеспечить оперативность их получения.

Основными задачами, успешно решаемыми с использованием навигационных систем, позволяющих получить пространственно-временную информацию, являются задачи, прямо связанные с оптимизацией оперативно- служебной деятельности правоохранительных органов (автоматизированный контроль сотрудников, определение местонахождения сотрудников и транспортных средств, представление в графической форме информации о позиционировании сил и средств и т.д.).

Основные положения диссертационного исследования Н. Ю. Дусевой сводятся к следующему:

1. **Понятие глобальной навигационной системы, включающей методы, а также программные и технические средства, позволяющие организовать фиксацию, обработку и получение пространственно- временной информации правоохранительными органами**.

Глобальная навигационная система — это совокупность методов, программных и технических средств, позволяющих организовать фиксацию пространственно-временной информации и получение ее правоохранительными органами. Целью создания данной системы является повышение уровня информационно-аналитического обеспечения деятельности правоохранительных органов при осуществлении расследования и предупреждении преступлений.

2. **Структура и связи между составными элементами глобальной навигационной системы**.

Глобальная навигационная система представляет собой совокупность средств получения, а также программно-аппаратных комплексов обработки и передачи пространственно-временной информации. Комплекс средств получения пространственно-временной информации включает в себя следующие подсистемы:

- ГЛОНАСС,
- подсистему стационарной связи,
- подсистему мобильной связи,
- подсистему радиочастотной идентификации,
- подсистему видеофиксации,
- подсистемы фиксации фактов обращения и персонализации.

Программно-аппаратные комплексы обработки и передачи пространственно-временной информации направлены на автоматизацию решения задач по организации хранения, передачи, структурирования и обеспечения возможности ее аналитической обработки.

3. **Перечень типичных следственных задач, решаемых с использованием ресурсов глобальной навигационной системы при осуществлении правоохранительной деятельности по расследованию и предупреждению преступлений**.

Анализ следственной практики и практики проведения оперативно-разыскных мероприятий позволяет выделить задачи, решение которых основано на использовании пространственно-временной информации, полученной средствами глобальной навигационной системы:

- установление фигурантов и возможных свидетелей преступления,
- розыск лиц,
- установление места совершения преступления,
- установление средств совершения преступления,
- установление алиби лица,
- розыск похищенного.

4. **Структура программно-технического комплекса, разработанного для получения, накопления, анализа и использования пространственно- временных данных об объектах, имеющих криминалистическое значение, полученных с помощью глобальной навигационной системы**.

Глобальная навигационная система, являясь потенциальным источником пространственно-временной информации об объектах и событиях, попавших в поле зрения правоохранительных органов, может быть отнесена к технико-криминалистическим средствам, заимствованным из других областей науки и техники и приспособленным для криминалистических целей.

Подсистемы, входящие в состав глобальной навигационной системы, отличаются набором фиксируемых данных, принципами работы, а также формой представления полученной информации. Для оптимизации комплексного использования составных частей глобальной навигационной системы необходима интеграция всех массивов пространственно-временной информации, зафиксированной их средствами, в единый информационный комплекс. Однако различия в принципах фиксации пространственно- временной информации в системах с автоматической фиксацией данных (ГЛОНАСС, стационарные системы связи, системы мобильной связи, системы радиочастотной идентификации, системы видеофиксации) и системах фиксации фактов обращения и персонализации диктуют необходимость разделения алгоритмов их использования в интересах правоохранительной деятельности.

Для того чтобы обеспечить оперативность получения пространственно-временной информации о контролируемых объектах, а также представление данной информации в удобном для визуального восприятия виде, необходима интеграция систем с автоматической фиксацией данных в единую структуру. Основой для данной интеграции могут служить существующие программно-технические комплексы систем мониторинга транспортных средств, функционирующие на основе спутниковой навигации, которая позволяет получать информацию о контролируемых объектах в виде карты с указанием их местонахождения в определенный момент времени. Одновременное отображение на карте местности пространственно-временной информации из всех систем с автоматической фиксацией данных позволит провести в процессе расследования преступлений анализ потенциальных источников криминалистически значимой информации, составить план последующих следственных действий.

С учетом назначения формируемой глобальной навигационной системы к перечню ее основных функциональных возможностей необходимо отнести:

- мониторинг контролируемых объектов;
- отображение местоположения контролируемых объектов на электронной карте местности;
- аналитическую обработку полученных данных.

После событий 11 сентября создан ряд интересных **технологий дистанционной слежки**, которые могут найти повсеместное применение.

После ликвидации Усамы бен Ладена командой американского спецназа SEAL Team 6 в поле зрения журналистов попала **секретная программа Пентагона** под названием **«Метки, отслеживание и поиск»,** или TTL. **Целью этого проекта является создание средств, которые позволяют выследить особо важных лиц, скрывающихся в районе боевых действий или даже среди населения другой страны**.

С момента подписания первого контракта в рамках этой программы с компанией Blackbird Technologies военные начали получать огромное количество новинок и перспективных разработок. В настоящее время арсенал средств слежки охватывает практически все возможные способы идентификации и сопровождения человека: **от классических сканеров отпечатков пальцев и радужки глаза до тепловой сигнатуры конкретного человека и микроскопической пыли, распыляемой с беспилотных самолетов и светящейся в лучах радаров**.

Антитеррористическая батарейка

Первой, достаточно простой, была **технология инфракрасных маяков**, которую используют как солдаты, так и секретные агенты. Маяк представляет собой программируемую ИК-лампу, работающую в импульсном или непрерывном режиме, и источник питания. Свет, излучаемый таким маяком, не виден невооруженным глазом, но хорошо заметен в прибор ночного видения (ПНВ) или тепловизор. В июне 2009 г. «Аль-Каида» выпустила электронную книгу, посвященную тактике шпионов из числа местного населения, которые работают на США. Среди описаний тактики действия вражеских агентов авторы из «Аль-Каиды» публикуют фотографии инфракрасного маяка, приспособленного для работы от обычной 9-вольтовой батарейки типа «Кроны», которую несложно купить в Пакистане. В книге утверждается, что эти устройства пакистанские шпионы, нанятые американцами, используют для наведения **беспилотных самолетов**. Возможно, имеется в виду, что агенты таким образом, практически ничем не рискуя и не связываясь со своими «работодателями», отмечают маяками автомобили и здания, где скрываются террористы.

Надо заметить, что похожие инфракрасные маяки используют и американские солдаты, для того чтобы пилоты вертолетов и операторы БПЛА могли отличить их от бойцов противника. Сегодня инфракрасные маяки уже морально устарели. Есть сообщения, что полевые агенты получили в распоряжение специальные мобильные телефоны, оснащенные встроенным инфракрасным лазером. В пыльном воздухе лазерный луч с большого расстояния виден в ПНВ или тепловизор, что позволяет агенту указывать на цель, не приближаясь к ней. Кроме того, такой «лазерный» телефон может в режиме реального времени давать целеуказание ракетам Hellfire, что потенциально снижает вероятность побочного ущерба.

Квантовая точка на карте

Чтобы отслеживать передвижение определенного человека и выделять его из толпы, американские военные разрабатывают специальную жидкость, которая позволяет обнаружить объект с большого расстояния.

Компания Voxtel подготавливает продукт под названием NightMarks. Он представляет собой прозрачную жидкость, состоящую из крошечных **нанокристаллических квантовых точек** на основе **селенида кадмия**. Этот материал способен поглощать ультрафиолетовое (200–400 нм) или инфракрасное (700–1600 нм) излучение, а затем эффективно передавать энергию на **специальные нанокристаллические люминофоры**, которые светятся как в видимой (400–700 нм), так и в ближней инфракрасной области спектра.

Достаточно нанести такую жидкость на одежду или кожу человека (простым рукопожатием, с помощью БПЛА или другим способом) — и беспилотный разведчик сможет надежно отслеживать яркую метку с большого расстояния. Эффектами поглощения и испускания света можно управлять, что позволяет изменить оптические свойства квантовых точек и создать множество своеобразных спектральных штрих-кодов. Таким образом, появляется возможность отслеживать и надежно идентифицировать множество объектов.

Компания Tiax работает над аналогичными метками, которые могут со временем разлагаться. Это позволит избежать путаницы в большом количестве объектов наблюдения, а также снизить вероятность обнаружения факта слежки.

Использование RFID-чипов

Они похожи на те, что применяются для метки товаров в магазинах. В настоящее время армия США уже широко использует эту технологию для идентификации своих сил на поле боя и для логистики.

Специалисты Sandia National Laboratories разработали RFID-метки, которые способны реагировать на радиолокационный импульс и с высокой точностью определять местоположение объекта слежки. Например, обычные чипы, используемые в магазинах, имеют дальность действия в несколько метров, в то время как у RFID-меток от Sandia радиус до 20 км. Особенностью технологии является высокая скрытность: метки «отзываются» только после облучения специальным радиолокационным импульсом.

Подобные RFID-чипы можно использовать не только для оперативной слежки за людьми и автотранспортом, но и в качестве превентивной меры по контролю за оружием, например, встраивать их в переносные зенитные ракетные комплексы или противотанковые ракеты. В случае попадания этого оружия в руки террористов его будет достаточно легко обнаружить и быстро уничтожить ракетным ударом.

Миниатюрные RFID-метки могут работать с компактными радарами вроде M600 SpotterRF. Прибор размером с ноутбук разработан прежде всего для охраны периметра военных баз, но имеет большой потенциал для скрытой слежки.

M600 использует радиоволны X-диапазона и может обнаружить пешеходов на расстоянии до 1 км, а автотранспорт — до 1,5 км. Радар оснащен датчиком GPS и интегрирован с сервисом Google Earth, что позволяет отслеживать местоположение объекта на интерактивной карте.

Технологии уникальных запахов

Технологии оптического и радиолокационного слежения совершенны, но потенциально обнаружимы и поддаются обратному инжинирингу, то есть враг может разобрать найденный маяк и придумать контрмеры.

По этой причине военные ищут дополнительные способы тайной слежки. Технология компании Tracer Detection Technology предполагает использование уникальных запахов, позволяющих безошибочно выделить искомый объект из толпы. Специалисты компании изобрели специальный парафиновый карандаш, наполненный перфторуглеродами — термически стабильными соединениями, которые используются повсеместно от производства холодильников до парфюмерии. Пары перфторуглеродов могут отслеживаться с помощью различных датчиков, например газового хроматографа. Достаточно провести карандашом по объекту слежки — и он в течение нескольких часов будет источать специфичный, незаметный для человеческого носа аромат. При этом маскировка в наглухо запертой комнате или под десятью слоями одежды не поможет: по данным исследования, представленного в Министерство юстиции США, перфторуглеродные маркеры проникают сквозь закрытые окна, контейнеры и запертые чемоданы. Остаточные следы маркера сохраняются даже после тщательного смывания.

Технологии биомаркеров

В 2007 г. на одном из брифингов Сил специальных операций США кратко упомянули об использовании в качестве технологии слежки биомаркеров — биологических веществ, которые позволяют надежно идентифицировать человека. Подробностей об этой технологии нет; судя по всему, она представляет собой протеин, в котором зашифрован определенный код-идентификатор.

На руке человека такая метка выглядит как обычный синяк, можно снять с себя всю одежду, тщательно вымыть тело и сбрить все волосы, но маленькая незаметная биометка позволит идентифицировать человека в любом случае. Тактика использования биомаркеров остается загадкой, особенно это касается считывания информации и внедрения биометки. Теоретически биомаркер может оставаться в человеке на всю жизнь, что позволяет быстро выявить террориста, который выдает себя за другого человека.

Технология трехмерного моделирования лица человека

Все описанные выше технологии имеют один существенный недостаток: нужно подобраться к преследуемому поближе. Однако это не всегда возможно.

Чтобы от подобного «невидимого ока» скрыться было совершенно невозможно, компания Photon-X разрабатывает **технологию трехмерного моделирования лица человека по нескольким снимкам с оптических и инфракрасных камер беспилотников**. Специальное программное обеспечение позволяет создать детальный профиль головы человека с помощью мультиспектральных датчиков и анализа движения лицевых мышц. Новая система позволит идентифицировать человека в толпе и сопровождать его без необходимости установки каких-либо маяков. Разумеется, оптические сенсоры не могут следить за человеком внутри здания, но зато они способны легко найти его даже на многолюдной улице большого города. Далее при необходимости врага можно уничтожить ракетой или привлечь агентов, которые установят маяк. Система Photon-X решает главную задачу — **слежение за большим количеством людей на обширных пространствах**.

Отдельным направлением геолокации является использование современных систем навигации и слежениия за наземными транспортными средствами на базе спутниковых технологий.

А. Б. Внуков, генеральный директор ООО «Геопарк», подробно рассказал об этом в своей статье на страницах журнала «Горная промышленность» (№ 6, 2006 г.).

Знание своего местоположения всегда было необходимым условием любой деятельности человека, связанной с перемещением (доставкой) грузов, путешествиями, военными действиями, оперативно-разыскной деятельностью. Из этих потребностей и выросла наука о навигации и появились различные навигационные приборы и средства — секстан, компас, карта и др. При этом самые совершенные и технически сложные средства навигации наибольшее распространение имели на море и в авиации. Наземным путникам в основном были доступны карты, компасы, а также одометры.

По мере развития новых средств навигации — инерциальных, радиотехнических, а также возрастания роли и объема наземных транспортных перевозок в повседневной жизни, современное навигационное оборудование постепенно стало появляться и на наземном транспорте.

Технология определения местоположения (позиционирования) является фундаментом построения систем навигации транспортных средств и систем слежения за ними. На наземном транспорте наиболее употребительными являются следующие методы местоопределения:

- маркерные (зоновые),
- одометрические (методы счисления пути),
- инерциальные,
- радиомаячные и радиопеленгационные,
- методы космической навигации.

С начала XXI века для определения местоположения наземных транспортных средств все более широкое распространение получают **методы космической**

навигации, основанные на использовании информации космических навигационных и навигационно-связных систем. Космические системы навигации и связи воплощают в себе последние достижения науки и техники и имеют глобальную зону действия, обеспечивая оперативность и высокую точность определения координат непосредственно на транспортном средстве. В космических навигационных системах в качестве ориентиров выступают космические аппараты, относительно которых с помощью специальной навигационных приборов проводятся измерения навигационных параметров.

Наибольшее применение получили космические навигационные системы GPS (США) и ГЛОНАСС (РФ). В настоящее время готовится к развертыванию и европейская космическая навигационная система GALLILEO. Системы ГЛОНАСС и GPS обеспечивают бесплатную глобальную всепогодную круглосуточную навигацию. Каждая из систем включает в себя орбитальную группировку (созвездие) навигационных спутников с высотой орбиты около 20 тыс. км. В отличие от системы GPS, имеющей полную орбитальную группировку (24 спутника), в составе отечественной системы ГЛОНАСС только 14 рабочих спутников — и это ограничивает ее возможности. Спутники непрерывно излучают навигационные радиосигналы. На транспортном средстве, где устанавливается навигационный приемник, принимаются сигналы одновременно с нескольких спутников каждой навигационной системы.

При наличии в зоне видимости одновременно четырех спутников в приемнике определяются координаты, высота, скорость, курс транспортного средства и текущее время. В качестве дополнительной информации для пользователя могут рассчитываться и предоставляться направление на очередную точку маршрута, пройденное и оставшееся расстояние до различных точек маршрута, время прибытия к цели, отклонение от заданного маршрута и пр.

Точность местоопределения обычных приемников любой из систем составляет 10–30 м. Предпочтительный выбор GPS-приемников связан в первую очередь с их невысокой стоимостью.

Следует отметить, что, кроме космических навигационных систем GPS и ГЛОНАСС, для определения местоположения достаточно широкое применение на наземном транспорте находит и **навигационно-связная система Euteltracs, в которой местоопределение осуществляется по измерениям относительно геостационарных спутников связи**.

Большинство современных систем навигации автомобиля включает электронный дисплей с картой-схемой автомобильных дорог и пиктограммами, указывающими текущее расположение автомобиля и адресата. Наиболее передовые системы также вычисляют оптимальные маршруты и используют упрощенную графику и/или синтезатор голоса, чтобы обеспечить выдачу подсказок в реальном масштабе времени, постепенно выдавая необходимые команды управления для достижения адресата.

На основе систем определения местоположения транспортных средств строятся системы слежения (мониторинга). Для этого навигационные данные от автомобильной навигационной системы передаются по каналу связи в диспетчерский центр в реальном масштабе времени или после завершения рейса. Полученные данные в диспетчерском центре отображаются на электронной карте местности, заносятся в базы данных и используются для управления перевозками.

Объединение навигационно-связного оборудования транспортных средств, канала связи и обмена данными, а также оборудования диспетчерского центра и образует систему слежения за транспортными средствами (в англоязычной аббревиатуре AVL — Automatic Vehicle Location Systems). В AVL-системах на основе спутниковых технологий на транспортном средстве устанавливается бортовой комплект в составе навигационного приемника GPS, ГЛОНАСС или GALLILEO, блока управления (контроллера), модема, средства связи и передачи данных (в простейшем случае — радиостанции).

Данные о текущих значениях долготы, широты, высоты, скорости и направления движения автомобиля, полученные от спутникового навигационного приемника или по запросу центра слежения (диспетчерского центра), по каналу связи (выделенному УКВ- или КВ-радиоканалу, транкинговой или сотовой системе связи) передаются в диспетчерский центр.

В центре слежения (диспетчерском центре) высокоточная информация о скорости и местоположении транспортного средства отображается на электронной карте. При этом имеется возможность в широком диапазоне менять масштабы карт, отображать текущее положение всего парка и отдельных объектов, видеть весь пройденный маршрут в динамике, с указанием времени и скорости, отображать объекты в различных цветах, масштабировать объекты и т.д. Это позволяет диспетчеру всегда знать текущее местоположение всех транспортных средств, прогнозировать время прибытия в пункт назначения, при необходимости корректировать маршрут движения транспортных средств и иметь двухстороннюю связь с водителем в любое время.

Получаемая в процессе слежения информация о местоположении, скорости и состоянии транспортного средства сохраняется в базе данных и может быть использована для послерейсового анализа.

Системы слежения за транспортными средствами по зоне действия условно можно разделить на:

- системы локального покрытия (до 50 км),
- системы регионального покрытия (более 100 км),
- системы глобального покрытия.

Размеры зоны действия систем слежения определяются как зоной действия подсистемы навигации, так и зоной действия систем связи. В системах слежения на основе спутниковых навигационных технологий зона действия целиком определяется дальностью действия используемых систем связи.

Для построения локальных систем слежения могут использоваться стандартные (Conventional) системы радиосвязи с использованием ретранслятора или без него. Если система использует прямой радиоканал на выделенной частоте, то радиус зоны охвата может составлять около 5–30 км в зависимости от используемой частоты и мощности передатчика, высоты подъема антенны передатчика и других условий.

Для построения локальных и региональных систем слежения также используются транкинговые и сотовые системы связи. В этом случае рабочая область системы слежения совпадает с зоной действия соответствующей сети связи.

Широкие перспективы в создании систем слежения открывает **использование сотовых сетей связи в режиме передачи данных**.

Системы слежения с глобальным покрытием применяются для контроля за транспортными средствами при междугородних и международных перевозках. Для этих систем могут быть использованы каналы спутниковых систем подвижной связи на базе геостационарных спутников или на базе низкоорбитальных спутников.

В настоящее время основная масса систем слежения для дальних перевозок использует системы на базе геостационарных спутников связи — Inmarsat и EutelTracs.

Международная система спутниковой связи Inmarsat разрабатывалась для военно-морского флота и морских перевозок, однако последняя реализация Inmarsat рассчитана также и на сухопутные транспортные средства. Зона обслуживания системы Inmarsat охватывает почти всю поверхность земного шара, за исключением околополюсного пространства.

Для контроля за местоположением транспортных средств и связи с ними при их нахождении в любой точке мира на транспортное средство устанавливается спутниковая станция Inmarsat со встроенным приемником GPS. По заданному интервалу или по запросу из диспетчерского центра информация с навигационного приемника GPS (географические координаты, скорость) в цифровом виде поступает в диспетчерский центр. Точность определения местоположения транспортного средства, как правило, не ниже 100 м. В диспетчерском центре происходит обработка поступающей от транспортных средств информации. Их местоположение отображается на цифровых электронных картах с одновременным занесением принятой информации в базу данных.

Возможен обмен текстовой информацией между диспетчерским центром и подвижным объектом, а также между подвижным объектом и сетями «Телекс», «Факс», X.25, X.400, Email, другими станциями системы Inmarsat. Также между транспортным средством и диспетчерским центром возможен обмен короткими текстовыми сообщениями, которые в автомобиле высвечиваются на индикаторе бортового компьютера.

Комбинированная система определения координат и связи EutelTracs была создана в 1992 г. на основе спутников связи EutelSat и в настоящее время используется

в Европе, Северной Африке и на Ближнем Востоке. Система EutelTracs разрабатывалась специально для наземного транспорта.

В состав сети EutelTracs входит центральная станция и станция маршрутизации («почтовый ящик» системы, расположенный во Франции), а также несколько спутниковых диспетчерских пунктов и мобильные терминалы. Связь с абонентами устанавливается с помощью спутниковых диспетчерских пунктов. Станция маршрутизации выполняет обработку сообщений и выдает разрешение на установление соединения. Диспетчерские пункты могут быть связаны со станцией маршрутизации по телефонным линиям общего пользования (PSTN) или по каналам сети передачи данных (PSDN). Определение местоположения транспортного средства осуществляется либо по измерениям относительно спутников связи EutelTracs, либо с помощью приемника GPS. Точность определения координат — порядка 100 м.

Для организации системы слежения на каждой автомашине устанавливается малогабаритный мобильный связной терминал (МСТ), состоящий из трех блоков: пульта водителя, связного блока и антенны. Рабочее место диспетчера представляет собой стандартный персональный компьютер и модем, обеспечивающий связь с региональным центром системы в Москве. Получение, регистрация и хранение информации ведется автоматически даже в отсутствие диспетчера на основе принципа «электронного почтового ящика».

При дополнительном оснащении мобильных терминалов системами телеметрии может вестись дистанционный контроль параметров транспортных средств и грузов. При возникновении на трассе чрезвычайной ситуации, когда срочно требуется помощь (авария или поломка транспортного средства, нападение или внезапная болезнь), водитель имеет возможность послать сигнал бедствия одним нажатием кнопки.

Вторым направлением создания систем слежения для дальних перевозок является **использование каналов низкоорбитальных систем подвижной спутниковой связи**. Основное отличие данных систем от геостационарных состоит в том, что их орбитальные группировки включают спутники с небольшой высотой орбиты (около тысячи километров). Это позволяет создать более дешевые и малогабаритные абонентские спутниковые терминалы.

В настоящее время в России представлена низкоорбитальная система связи Globalstar.

В состав системы спутниковой связи Globalstar входят 48 космических спутников связи, наземный сегмент, пользовательское оборудование. Система обеспечивает персональную связь в пределах от 70 градусов южной широты до 70 градусов северной широты.

Общий недостаток, объединяющий системы, использующие спутниковые каналы для передачи данных типа Inmarsat, EutelTracs или Globalstar,— это достаточно высокая стоимость бортового оборудования (свыше тысячи долларов США) и сравнительно дорогая абонентская плата за трафик.

Отдельно следует отметить устройства для реализации послерейсового контроля за маршрутом транспортных средств. По аналогии с авиацией эти устройства также названы черным ящиком.

Эта разновидность систем слежения является наиболее дешевой в реализации, поскольку отсутствуют дорогое связное оборудование и оплата трафика. Использование черного ящика позволяет транспортным предприятиям и компаниям составлять оптимальные задания на грузоперевозки, выявлять нарушения водителем путевого задания, решать спорные вопросы о режимах перевозки грузов (например, скоропортящихся грузов). При массовом использовании бортовых устройств регистрации на автотранспортных средствах полученные данные о маршрутах и режимах движения могут найти применение при разборе причин дорожно-транспортных происшествий.

Черный ящик стационарно устанавливается на транспортное средство и включается при начале движения (остановить его работу водитель не может). Черный ящик может также устанавливаться скрытно. По возвращении транспортного средства информация о пройденном маршруте считывается с помощью переносного компьютера или специального устройства для считывания. Информация о пройденном маршруте отображается на фоне электронной карты местности. Программное обеспечение позволяет также проанализировать прохождение маршрута:

- места/время остановок;
- показания датчиков (например, открытие дверей фургона или температура в рефрижераторе);
- уход с маршрута, запись маршрутов в базу данных, сравнение различных пройденных маршрутов и т.д.

Все это является неоценимой информацией для проведения различных оперативно-разыскных мероприятий (таких как контролируемая поставка).

Возможности программы спутникового слежения за мобильными телефонами

Современные GPS-технологии могут помочь выполнить **поиск телефона через спутник**, а также многие другие объекты. Осуществляет все это спутниковая система, работающая через специальную программу слежения (/gps/programma-slezhenija-za-telefonom) на телефонах фирмы Nokia, iPhone, HTC и на различных операционных системах, например Android, которая приобретает с каждым днем все большую популярность.

Если система слежения используется для наблюдения за людьми, то у объекта наблюдения с собой всегда должно быть специальное устройство — **персональный GPS-трекер или сотовый телефон фирмы Nokia, iPhone, HTC с поддержкой функции GPS или на системе Android.** Таким образом, этот мобильный телефон превратится в своеобразный «маячок» с установленной на

нем специальной программой слежения. Если использовать программу слежения для наблюдения за людьми, то мобильный телефон легко можно положить в портфель или карман объекта, который нуждается в вашем контроле, а если необходимо GPS-слежение за автомобилем, мобильный телефон можно положить и в бардачок. После определения программой слежения точных координат, местонахождения и скорости информация отправляется на сервер системы. Все эти данные программа получает с заранее заданной периодичностью.

Увидеть то, как проводится GPS-слежение, можно в режиме онлайн: с компьютера или мобильного телефона. Помимо местонахождения объекта наблюдения в настоящий момент, эта GPS-программа позволяет на электронной карте проследить направление движения и скорость. Система слежения GPS сохраняет всю историю передвижений отслеживаемых объектов.

Сегодня каждый желающий, вооружившись специальным программным обеспечением, имеет возможность проследить за действиями любого абонента сотовой связи.

То есть при помощи специальных программ, таких как ShadowGuard, например, можно прослушать переговоры по чужому телефону или же прочитать переписку по СМС. Еще несколько лет назад это было похоже на шпионскую фантастику, но сегодня это реальность, и уже огромное количество людей воспользовалось этим. А там, где имеется спрос, как известно из законов рынка, рождается и предложение. И на сегодняшний день появилось множество сервисов, которые предлагают воспользоваться такой невероятной возможностью.

Мы привели в качестве примера программу прослушивания мобильного телефона ShadowGuard и будем использовать этот пример и дальше для того, чтобы раскрыть основные возможности подобного шпионского программного обеспечения. Одним из самых востребованных запросов является прослушивание сотового телефона.

При установке программы на телефон все данные передаются в личный кабинет пользователя программы. Таким образом, все изменения в данных, которые происходят на прослушиваемом телефоне, передаются на сервер. Профессиональное средство прослушки, которым является программа ShadowGuard, позволяет не только следить за информацией на другом телефоне, но и управлять некоторыми функциями — например, блокировать входящие и исходящие сообщения и звонки. Для того чтобы прослушивание сотового телефона и другие возможности программы были доступными, сначала необходимо пройти регистрацию на сайте программы. И после активации пользователь получает доступ к данным на интересуемом телефоне.

Саму программу необходимо скрытно установить на чужой телефон. Здесь пользователь должен проявить настоящую оперативную смекалку и находчивость. Зато при успешно проведенной операции он будет щедро вознагражден: в его распоряжении окажется вся информация — адреса электронной почты,

телефонная книжка, переписка. При работе на чужом телефоне программа никак себя не обнаруживает. Замечательно то, что в такой программе есть возможность прослушивать сотовые телефоны бесплатно, установив бесплатный модуль. В режиме тестирования функционал программы ограничен.

В начале XXI века возникла тотальная система наблюдения за человеком, которая преследует ребенка и взрослого, живого и мертвого. Одно дело, когда источники информации существовали отдельно, в разных органах и организациях, и другое — когда их можно собрать воедино, проанализировать и составить информационный портрет человека. Такая уникальная возможность появилась с созданием новейших информационных технологий, базирующихся на электронных устройствах, которые произвели революцию в сборе всех данных от наблюдения за человеком, причем в тайне от него. Эту информацию можно передать безвозмездно или продать, в то время как источники этой информации — частные лица — даже не подозревают об этом процессе.

Электронное антитеррористическое наблюдение

Серьезный шаг сделали и разведывательные технологии после событий 11 сентября 2001 г., когда были приняты беспрецедентные меры, охарактеризованные в СМИ как конец существования конфиденциальной информации в США. Особого внимания заслуживает крупномасштабный проект Министерства обороны США «**Тотальная информационная осведомленность**» (ТИО). Он предполагает разработку и эксплуатацию новейших информационно-компьютерных технологий, с помощью которых можно осуществлять тотальное наблюдение за счет массированного увеличения источников информации, перехвата сообщений любого характера, оперативного анализа в режиме реального времени, то есть сбора колоссального количества данных, а главное — молниеносную реакцию спецслужб. Как утверждается, эти меры будут противодействовать террористическим угрозам за счет «мониторинга местонахождения, передвижений и деловой активности населения, то есть сбора максимально широкой информации обо всех подозрительных явлениях, указывающих на планы террористов».

Система ТИО интегрирует всеобъемлющие цифровые данные об американских гражданах, а также об иностранцах, имеющих контакты с населением США, которые следует подразделить на два типа: а) личностные, деловые, функциональные; б) биометрические. Первые предполагается черпать из всех существующих баз данных как государственного, так и отраслевого назначения: медицинских, образовательных, торговых, туристических, телефонных, корпоративных, ветеринарных и т.д.; из источников, куда проникли все отслеживающие электронные устройства: банковские счета, кредитные карточки, сервисы по аренде машин, транспортные агентства; а также из медицинских и ветеринарных записей, из телефонных и иных коммуникативных сообщений,

из письменных, электронных, телефонных заявлений граждан в госорганы и т.п. Биометрические данные — это изображение радужной оболочки и сетчатки глаз, отпечатки пальцев, ДНК, графические снимки лица и т.д.

Если учесть, что при этом используется хорошо зарекомендовавшая себя традиционная техника сбора данных (например, «просеивание» телефонных счетов, магазинных дисконтных карточек и т.п. через виртуальное «сито»), то сбор информации по линии ТИО достигнет беспрецедентных масштабов. Возникнет уникальная централизованная система, которая, преодолев разобщенность и недостатки многочисленных имеющихся баз данных, будет содержать точные данные, где находился и что делал конкретный человек в заданное время. И тогда каждый гражданин США — будь то потенциальный террорист или лояльный гражданин — окажется под информационным колпаком спецслужб.

Новый этап в эпоху слежения за объектами связан с космическими летательными аппаратами, в частности спутниками, возможности которых с учетом постоянно совершенствующейся фотовидеоаппаратуры безграничны. Причем передающие спутники могут двигаться по определенной траектории, фиксируя все на своем пути, а стационарные — предметы и их передвижение в одной географической точке. Спутники, оснащенные специальными приборами, не только «видят», но и «слышат», отслеживая разнообразные коммуникативные процессы. Это своеобразные динамические базы данных: они не только собирают и хранят информацию, но и могут отправлять ее на землю в заданном режиме. Наличие кода предохраняет ее от расшифровки. Спутникам мирного назначения проложили дорогу спутники-шпионы, существующие уже более 40 лет, но несущие свою службу и сейчас. Они оснащены обычными или инфракрасными фотокинотелекамерами, электрооптическими сканерами и иной аппаратурой.

Вся Земля находится в зоне видимости космических аппаратов. Маршруты спутников ничем не ограничены, поэтому с их помощью любое государство способно заглянуть в «огород» соседа, причем не одномоментно, а постоянно и в любое время. Вероятно, с точки зрения военных и политических целей (например, контроль выполнения двусторонних или многосторонних государственных обязательств) они вряд ли заменимы.

В ряде стран, в первую очередь в США, созданы **системы геопространственной разведки** — прежде всего в целях национальной безопасности, а также для использования в гражданских нуждах. Спутниковая геопространственная информация находит применение и в борьбе с терроризмом.

В Германии введена **единая компьютерная антитеррористическая база данных**. Этот информационный банк состоит из двух частей — основной и расширенной. В основную включен набор данных, необходимых для идентификации личности: имя, пол, дата рождения, адрес, гражданство, владение языками, цветное фото и приметы подозреваемого в террористической деятельности.

Доступ к этой информации имеют все разведывательные органы и службы по борьбе с преступностью.

В расширенную базу внесена информация о семейном положении подозреваемого; его профессии, образовании, конфессиональной принадлежности; номерах автомобиля, банковского счета и телефона; данные о передвижении по миру; навыках владения оружием и обращения со взрывчатыми веществами; круге общения, связях с террористическими ячейками, принадлежности к террористическим ячейкам. Эту информацию заинтересованные ведомства могут получить по специальному запросу. Однако, во-первых, субъекты таких запросов строго не оговорены. В результате чего запрос могут организовать и сами террористы, выявив тем самым круг потенциальных сторонников и недоброжелателей. А во-вторых, возможны утечка информации изнутри и взлом извне или то и другое вместе. Тогда тщательно собранная всеобъемлющая информация может оказаться во власти посторонних людей, а главное — криминальных структур. Нетрудно представить удовлетворенность последних, когда нужные сведения будут поданы буквально на блюдечке.

Разведывательные системы становятся все более универсальными: в автоматическом режиме они не только собирают информацию, но и осуществляют ее анализ, делают выводы. Именно так работают системы глобальной слежки: в ряде англоязычных стран — ECHELO, в Европе — ENFOPOL, в России — СОРМ-2.

Революционным событием является возникновение возможности с помощью современных информационно-компьютерных технологий обозревать не отдельные участки и регионы, но и целиком планету. Совсем недавно произошел беспрецедентный в мировой истории случай, когда известная компания Google Earth выставила на сетевое обозрение все без исключения уголки планеты. Появилось множество информации об объектах, о которых никто не ведал, в том числе и о тех, которые скрывались, например о секретных базах, аэродромах, кораблях, подлодках и т.д. Посредством новейших просматривающих устройств современное человечество, наконец, сумело увидеть свою колыбель и место обитания — Землю — в зеркале, называемом электронной информацией.

На повестке дня встал вопрос о **проблеме имплантации чипов, способных давать информацию о человеке везде и в любое время суток**. Комиссия Евросоюза 16 марта 2005 г. согласилась с заключением № 20 Европейской группы по этике в науке и новым технологиям, заявив, что использование электронных имплантатов для слежки за людьми законно, если такой контроль будет закреплен законодательно.

Также постоянно и **целеустремленно ведут сбор информации корпорации**, причем в двух направлениях: внешнем и внутреннем. Внешнее предполагает получение данных за пределами организации, а именно: данные о политической и экономической обстановке в мире, состоянии глобальных и региональных рынков, активах и намерениях конкурентов и т.д. В целом это колоссальный

объем информации; при современных масштабах транснациональных корпораций он превосходит данные, получаемые некоторыми государствами. Особое значение придается информации о потребителях продукции. В связи с этим следует обратить внимание на термин «протокол» (Д. Бурнам), который с помощью электронных устройств автоматически фиксирует самые обычные действия людей. Протокол всегда начеку. Он точно отмечает момент звонка человека по телефону, обналичивание им чека, использование кредитной карточки, покупку товара в магазине, взятие напрокат автомобиля, наконец, включение канала кабельного телевидения. Человек совершает множество и других обыденных действий, не заботясь о последствиях. А все это находит отражение в протоколах.

Распознавание лиц преступников и террористов, поиск пропавших людей на базе нейронных сетей

Почему технологии распознавания лиц будут все более востребованы в системах безопасности? Зачем помнить постоянно растущее количество паролей для разных сервисов и придумывать все более сложные способы идентификации себя в интернете, когда у каждого человека с рождения есть уникальный идентификатор — его лицо? Крупнейший онлайн-торговец, китайская Alibaba Group, в 2015 г. объявил о скором запуске системы Smile to Pay, которая позволит покупателям входить на сайт и подтверждать покупки, глядя в камеру смартфона. И это лишь одно из множества перспективных направлений технологии распознавания лиц.

В вопросах распознавания лиц для обеспечения безопасности железнодорожного транспорта главным экспертом может выступить **Япония**. Именно в этой стране в сферу рельсовых перевозок людей и грузов внедрено максимальное количество высокотехнологичных решений. И это при том, что Япония считается мировым лидером по объему пассажиропотока, проходящего через вокзалы (а вокзалы здесь зачастую объединяют и наземный, и подземный транспорт). Однако метрополитен Страны восходящего солнца, и в частности Токио, вывели в авангард очень печальные события. Система безопасности в столичной подземке кардинально обновилась после марта 1995 г., когда религиозные фанатики из секты «Аум Синрике» распылили на двух станциях ядовитый газ. Теперь *токийское метро буквально напичкано современными видеокамерами: на 290 станций их приходится несколько тысяч! Установлены камеры и во многих вагонах скоростных поездов. Также есть камеры, которые специализируются на вычленении предметов и людей, не двигающихся в течение долгого времени. Все видеозаписи поступают в единый ситуативный центр, куда стекается также вся информация от патрулирующих метро полицейских. Кроме того, имеются и специальные стереовидеокамеры, способные засечь посторонний предмет или человека на путях, и скомандовать поезду остановиться.*

В 2012 г. *Хитачи Кокусай Электрик* представила систему с камерой скрытого слежения, позволяющую обрабатывать базу данных *из 36 миллионов лиц за 1 секунду*.

Согласно заявлениям Хитачи, «эта высокая скорость обнаружения достигнута распознаванием лиц путем распознавания картинок на этапе записи камеры наблюдения и группировки полученных похожих лиц». Система объединяет лица, которые поворачиваются в рамках 30 градусов и имеют минимальный размер на картинке в 40×40 пикселей.

Планируется, что система скрытого видеонаблюдения будет внедряться в больших корпорациях, на крупных вокзалах и заводах. Применение такой системы в аэропорту или на вокзале поможет обнаружить злоумышленников, чьи фотографии заранее занесены в базу данных как «находящиеся в розыске».

В 2014 г. ФБР США объявило об успешном запуске в эксплуатацию *системы распознавания нового поколения (NGI)*. Ее целью является расширение возможностей ведомства по идентификации граждан, и она должна заменить старую, основанную исключительно на отпечатках пальцев. С 2011 г. система работала в экспериментальном режиме.

Основной особенностью NGI является то, что она получает и обрабатывает биометрические данные автоматически. Система работает за счет информации, получаемой с камер видеонаблюдения по всей стране. Она выявляет уникальные черты лица того или иного человека и сохраняет их в базе данных. Затем при расследовании преступления она сможет провести быстрый анализ снимков и обнаружить злоумышленников.

Для идентификации человека достаточно обнаружить, например, характерный шрам на его лице или татуировку на теле.

ФБР разработало NGI совместно с Lockheed Martin, Security Solutions и IBM. Целью программы назвалили «борьбу с терроризмом и преступностью благодаря улучшению способов биометрической идентификации, а также выработке новых методов анализа архивной информации в результате исследований, оценки и применения перспективных технологий».

С помощью этой системы в теории можно распознать человека на любой фотографии, если информация о нем содержится в базе данных. Подобные, но менее комплексные методы идентификации давно используют такие компании, как Facebook — их технологии позволяют автоматически идентифицировать того или иного пользователя на загруженной в социальную сеть фотографии. Проект разработки NGI рассчитан на десять лет, и в него вложено 1,2 млрд. долларов. О старте программы официально объявили в 2008 г., когда ФБР заключило первый контракт на ее реализацию с фирмой Lockheed Martin.

В 2011 г. система автоматического распознавания лиц начала функционировать в экспериментальном режиме. Правоохранительные органы США получили от ФБР программное обеспечение, которое позволяло мгновенно сравнивать

фотографии подозреваемых с базой данных. Число американских ведомств, использующих ее, постоянно растет.

NGI позволяет вести наблюдение за людьми, занимающими ответственные должности. К ним, например, относятся кассиры, учителя, работники социальных служб — то есть те, кому необходимо сдать отпечатки пальцев и фотографию при приеме на работу. Система позволяет правоохранительным органам каждого штата в течение 24 часов узнать, не совершил ли человек, претендующий на такую должность, какое-либо преступление. ФБР только предупреждает местные правоохранительные органы о том, что соискатель уже был однажды арестован, а дальше им предлагается принимать решение, что с ним делать, самостоятельно.

Эта система помогает также следить за гражданами, освобожденными из мест заключения досрочно. Если бывший арестант совершит преступление в одном штате страны, то эта информация очень быстро будет доступна властям остальных.

Помимо распознавания лиц, NGI способна идентифицировать человека по его зрачку. В последнее время фотографии зрачков заключенных активно собирают в американских тюрьмах. В теории они могут использоваться для идентификации злоумышленников на месте преступления.

Пока что NGI далека от совершенства. Низкая разрешающая способность большинства камер видеонаблюдения не позволяет системе эффективно распознавать лица людей и тем более их зрачки. Но ее использование приносит плоды уже сейчас.

Системы идентификации нового поколения ведут поиск лиц по базе с фотографиями более 50 млн. граждан.

В штате Нью-Йорк система распознавания лиц уже работает в Управлении автотранспорта. Благодаря ей власти арестовали более 100 человек и открыли почти 1000 расследований.

В США в июне 2017 г. начались первые испытания системы распознавания лиц в нескольких аэропортах. Пассажирам *авиакомпании JetBlue Airways*, ставшей инициатором эксперимента, не приходится даже доставать свои паспорта и прочие документы, чтобы попасть на борт самолета. Ведь новой системе достаточно бегло взглянуть на лица людей, чтобы проверить их через базы данных служб безопасности и зарегистрировать на рейс. Для того чтобы воплотить этот проект в жизнь, JetBlue Airways объединила усилия с Таможенной службой и Пограничным патрулем США. За программную сторону проекта отвечает компания SITA.

Работа новой системы основывается на сверке лица человека с хранящейся в базе данных фотографией. Людям не нужно предъявлять вообще никаких бумаг или заранее регистрироваться, чтобы принять участие в этой программе. В процессе распознавания человеку всего лишь нужно встать напротив камеры, которая моментально отсканирует лицо и сверит его с базой данных.

Другая американская авиакомпания — *Delta Air Lines* — тоже собирается использовать распознавание лиц для упрощения аэропортовой рутины. На этот раз биометрический сканер будет применяться на стойках сдачи багажа.

После печати ярлыка, который прикрепляется на сумку или чемодан, пассажира пригласят к автомату, оборудованному технологией распознавания лица, для сканирования и сверки с фотографией в документах.

Delta вложила в автоматизированную стойку регистрации багажа 600 тыс. долларов. На эти средства в международном аэропорту Миннеаполис/Сент-Пол летом 2017 г. установлены четыре подобных автомата.

Технологией заинтересовалась и *Австралия*. К 2020 г. страна планируетв вести биометрическую проверку пассажиров во всех австралийских аэропортах, включающую сканирование отпечатков пальцев и лица. Несмотря на то, что единой биометрической системы пока нет, потенциально в базу данных можно загрузить *всю информацию о путешественниках, включая сведения о билетах, туристическую историю, возможные судимости и пр.*

В будущем искусственный интеллект на основе этих данных сможет определять, представляет пассажир угрозу или нет. Испытания системы пройдут в аэропорту Канберры, столицы Австралии. Целью проекта является *автоматизация проверки 90% пассажиропотока*.

Подобные испытания в этой области проводят *финская авиакомпания Finnair, голландская KLM, а также международный аэропорт Париж — Шарль-де-Голль*. В некоторых случаях система распознавания лиц будет только дублировать действия сотрудников службы безопасности, так как на настоящий момент она не показывает 100%-ного результата и иногда неточна.

На Чемпионате мира по футболу — 2014 в Бразилии полиция была оснащена *солнечными очками со скрытыми камерами*, которые отслеживали и идентифицировали по криминальной базе до 400 пар глаз в секунду на расстоянии до 12 миль (оптимизированы для работы на расстоянии 50 м). Очки — скрытая камера подключены по беспроводной сети к базе данных, которая сравнивает лица с профилями 13 млн. эталонов и воспринимает 46 тыс. точек на лице для распознавания и идентификации совпадения.

Очки — скрытая камера могут не только идентифицировать преступников, но и отображать полицейскому дальнейшие указания к действию на мероприятии.

Ученые Института Макса Планка в Саарбрюккене (Германия) демонстрируют способ идентификации человека по нескольким фотографиям, даже если на большинстве из них его лицо закрыто. Разработанная исследователями система, которую они называют **«безликая система распознавания»**, тренирует нейронную сеть с помощью множества фотографий, содержащих как закрытые, так и хорошо видимые лица, а затем использует эти знания, чтобы идентифицировать человека с закрытым обличьем, ища сходства в области головы и на других участках тела.

Точность системы меняется в зависимости от того, сколько есть фотографий в наборе с хорошо видимым изображением лица. Даже тогда, когда есть только 1,25 копий изображений полностью видимого лица человека, система способна идентифицировать скрытые от обзора лица с точностью 69,6%; если есть 10 В Швеции компания Axis создала *первый в мире умный кодек (программный преобразователь сигнала*), созданный для IP-видео и IP-видеонаблюдения. Камера служит лишь первым звеном: не только воспринимает и транслирует, но и интеллектуально обрабатывает изображение. Большое количество охранных агентств используют технологии аналитики как начальный уровень защиты, особенно ночью.

К 2020 г., ожидают в Axis, в видеонаблюдении предстоит все еще развивать качество изображения и светочувствительность. Но одновременно *появятся камеры со встроенными системами аналитики или же со средствами передачи метаданных другой системе (метаданные — это, например, любые косвенные сведения о состоявшемся контакте двух лиц: кто и с кем, когда, где, сколько длился, какой была тема и т.п.).*

В Axis полагают, что сегодня есть три больших макротренда, которые следует связать. Это технологии Big Data, интернет вещей, а также облачные решения. В числе продвинутых технологий называют систему контроля доступа, сетевую систему контроля дверей, IP-аудио.

Одним из самых важных новых направлений Axis считают замену панорамных камер PTZ-камерами начального уровня. Угол обзора у такого прибора составляет 360 градусов, и он один может заменить сразу четыре камеры. Еще одно новшество — мультисенсор. Мультисенсорная камера, которая имеет угол обзора 180 градусов, появилась около года назад, но сейчас выпускаются и камеры с углом обзора 360 градусов. Они позволяют следить за дорогой, за площадью, за зданием.

Французская компания Orange Labs разработала алгоритм, способный *искусственно состаривать и омолаживать изображения лиц* на фотографиях и устанавливать их сходство с изображением на исходном фото. Это первый алгоритм, который генерирует высококачественные изображения лиц в любой заданной возрастной группе с сохранением узнаваемости человека. Для его создания исследователи использовали две *генеративные состязательные нейросети*.

В процессе обучения нейросети проанализировали, как выглядят лица шести возрастных категорий (до 18 лет, 19–29 лет, 30–39 лет, 40–49 лет, 50–59 лет и старше). Для этого в них загрузили по 5 тыс. фотографий людей из каждой возрастной категории. Таким образом, нейросети узнали паттерны изображения, характерные для определенного возраста, и смогли применить их для состаривания и омоложения изображения любого лица.

Обученный алгоритм ученые испытали на 10 тыс. изображений из базы IMDB-Wikipedia, а затем проверили результат с помощью программы, которая

сравнивает две фотографии и определяет, изображен ли на них тот же человек. В 80% случаев программа сумела идентифицировать людей, которых искусственно изменили на фото.

Технологию можно применять для розыска пропавших много лет назад людей, а также лиц, скрывающихся много лет от правосудия.

Китайская компания Baidu, занимающаяся созданием web-сервисов, в начале 2017 г. успешно использовала технологию искусственного интеллекта для поиска человека. Пропавший ребенок воссоединился с семьей спустя целых 27 лет.

Специалисты Baidu воспользовались программой распознавания лиц для того, чтобы вычислить местонахождение потерянного ребенка. Специалистам удалось выяснить, что 33-летний мужчина по имени Фу Гуи — это и есть маленький мальчик, похищенный возле школы в далеком 1990 г.

Фу Гуи, как и его настоящая семья, был зарегистрирован на ресурсе Baidu. Мужчина выложил в Сеть свое фото в 10 лет, а его родители искали по фотографии четырехлетнего мальчика. Именно эти снимки и сопоставил искусственный интеллект. Кровное родство было подтверждено с помощью теста ДНК.

Компания Baidu использует базу из 200 млн. изображений, для того чтобы совершенствовать работу системы распознавания лиц. Глава компании Baidu Робин Ли внес предложение о создании централизованной базы данных со сведениями о пропавших детях, чтобы помочь воссоединиться еще многим семьям.

Еще в 2010 г. в России создана первая *полностью отечественная биометрическая система моментального распознавания личности в толпе*. Разработана она компанией-интегратором «Техносерв» и называется «Каскад-Поток». Система ничем не уступает зарубежным аналогам. Она идентифицирует личность в режиме реального времени путем сопоставления видеоданных, полученных, например, с камер видеонаблюдения, с изображениями в базах данных оперативных учетов. На все это уходит лишь доля секунды, а вероятность правильного распознавания достигает 94%.

В 2013 г. в петербургском метро в дополнение к уже действующим камерам, пунктам досмотра и рамкам-металлодетекторам появилась «интеллектуальная» система видеонаблюдения. Базируется она на *комплексе КАРС (комплексной автоматической розыскной системе*), которая, в свою очередь, базируется на системе «Интеллект», разработанной ФСБ России для розыска преступников. Решение состоит из сети видеокамер и серверов для обработки информации. Опираясь на биометрические данные, система способна автоматически распознавать людей в толпе и анализировать их сходство с лицами, занесенными в базу данных преступников и подозреваемых. Если сходство превышает 90%, система оповещает об этом полицейских. Мало того, система даже умеет следить за потенциальным правонарушителем с помощью нескольких камер.

Московский метрополитен, который называют одним из самых уязвимых среди соизмеримых с ним объектов по объему пассажиропотока, тоже

в последние годы совершенствует систему безопасности. Уже создано **единое информационное радиопространство**, позволяющее сотрудникам подземки быстро связываться со службой охраны; станции и поезда оборудованы системой видеонаблюдения; на платформах установлены колонны экстренного вызова. Планируется **оснастить каждую станцию дополнительными камерами**, а также турникетами, способными распознать взрывные устройства, опасные предметы, отравляющие и радиоактивные вещества.

Заслуживает внимания и *аппаратно-программный комплекс биометрической идентификации лиц, находящихся в розыске или представляющих оперативный интерес для органов внутренних дел (АПБИ «АТИГ»)*, который, кроме лицевой геометрии, при распознавании использует все четыре основных алгоритма биометрической идентификации, известных науке на сегодняшний день:

- алгоритм векторного сравнения (VFA);
- алгоритм сравнения иерархических графов лица (HGM);
- алгоритм анализа локальных особенностей лица (LFA);
- алгоритм анализа структуры кожного покрова лица (STA).

Этот аппаратно-программный комплекс разработан *компанией «НТК ПрофИТ»*, установлен транспортной полицией в инициативном порядке в аэропорту Белгорода и с осени 2014 г. введен в эксплуатацию. Видеокамеры этого комплекса расположены на контрольном пункте, и система фиксирует всех пассажиров, пересекающих контрольный рубеж. При выявлении признаков сходства проходящего пассажира с разыскиваемым преступником (находящимся в розыске не только за преступления террористического характера, но и за иные противоправные деяния) система сигнализирует об этом сотрудникам полиции.

Уже первые месяцы эксплуатации аппаратно-программного комплекса принесли положительные результаты в отождествлении лиц, находящихся в федеральном розыске.

Российская компания «Вокорд» выпустила собственную систему дистанционного биометрического распознавания лиц *Vocord FaceControl.* «Вокорд» до сих пор работает с сервисами и устройствами, не связанными с распознаванием лиц.

Vocord FaceControl 3D работает с синхронными изображениями со стереокамер, строит 3D-модель лица в кадре (это занимает меньше секунды) и автоматически ищет совпадение полученной модели с моделями в имеющейся базе данных. Можно сопоставить 3D-модель и с обычными фото. Разработку проекта Vocord FaceControl 3D «Вокорд» начал с двухмерного распознавания лиц и сразу столкнулся с проблемой. Если человек отворачивался от камеры больше чем на 15 градусов в любой плоскости, построить модель лица уже не удавалось. Поэтому инженеры «Вокорда» разработали систему, которая на основе синхронных снимков с нескольких камер строит трехмерную модель лица. Эта модель сравнивается с фотографией на пропуске или в доступной базе, система идентифицирует личность человека на снимке и сохраняет модель в архиве.

Но даже с переходом на 3D-моделинг получению хорошего качества снимков мешало плохое качество съемки стандартных обзорных камер. Крупным компаниям невыгодно было разрабатывать и производить камеры только для распознавания изображений — ниша была слишком узкой.

«Вокорд» разработал свою технику на стыке классических обзорных камер и камер машинного зрения, которые обладали высокой чувствительностью, адаптировались к освещению, автоматически управляли объективом и делали снимки более четкими. Клиенту предлагался не отдельный софт, а полноценный аппаратно-программный продукт — тогда это было прорывом в области распознавания лиц.

В России у «Вокорда» несколько конкурентов в области технологий распознавания лиц: VisionLabs, «Техносерв», «Стилсофт» и «Смиларт».

«Вокорд» и «Техносерв» работают на одном поле, но «Вокорд» — это в первую очередь разработчик ПО, а «Техносерв» — интегратор, поэтому пространства для маневров на рынке достаточно, считает начальник отдела подготовки биометрических решений «Техносерва» Иван Тихонов. Но, как и «Вокорд», «Техносерв» ориентирован в основном на большие, комплексные проекты для крупных государственных и коммерческих структур.

Первые технологии распознавания лиц появились вместе с распространением фотографии и использовались для идентификации и поимки преступников. Об автоматизации речи не шло: лицо подозреваемого с изображенным на снимке преступником сверял человек. В середине 1980-х гг. стали широко использоваться компьютерные технологии и распознавание вышло на новый уровень: на снимке лица выделялись биометрические точки, расстояние между которыми измерял компьютер. Главным критерием был набор цифр, который получали путем деления длин отрезков, соединяющих эти точки. Затем к биометрическим точкам добавились уникальные признаки человеческого лица, что значительно облегчило процедуру распознавания; появились полностью автоматические системы. В 1990-х гг. оформилась четверка компаний — лидеров в этой сфере: немецкая Cornitec Systems, немецкая Neven Vision (купленная Google в 2006 г.), американская LI Identity Solutions и японская NEC.

Но за последние десять лет технология очень изменилась: для распознавания лиц начали использовать искусственные нейронные сети — математическую модель, построенную по принципу организации сетей нервных клеток живого организма. В процессе обучения нейронной сети задействованы две ее способности: запоминание (когда сеть дает верный отклик на входные данные) и обобщение (когда сеть выдает правильные результаты в ответ на входные данные). Именно эти свойства позволяют новейшей системе автоматически сравнивать новое изображение (фотографию или 3D-модель лица) с тем, что уже есть в ее базе.

Российская компания NTechLab победила в конкурсе алгоритмов распознавания лиц Megaface, организованном Вашингтонским университетом.

Основатель компании — выпускник факультета вычислительной математики и кибернетики МГУ им. М. В. Ломоносова Артем Кухаренко. Участвовать в конкурсе можно было в двух категориях, в каждой из которых предлагалось анализировать по два пакета: больше 500 тыс. изображений и меньше 500 тыс. изображений. NTechLab победила в двух соревнованиях и заняла 2-е место еще в двух.

Продукт NTechLab называется FaceN. Компания на сайте указывает, что он уже используется для поиска людей по фотографии и контроля доступа. Чтобы идентифицировать человека по фото, алгоритм должен уметь выделять такие черты лица, которые не зависят от того, как меняется внешность человека и как по-разному его можно сфотографировать. FaceN построен на так называемых инвариантных признаках — таких, которые характеризуют индивидуальное строение лица и не изменяются. При этом часть признаков (величина глаз, фактура бровей, форма губ) человеческий глаз распознает, а часть — выделить неспособен, указывают создатели технологии.

Сегодня система распознавания лиц применяется *в борьбе с криминалом*. Фоторобот преступника сверяется с изображениями в базах данных, либо производится съемка человеческого потока в людных местах, и лица людей в реальном времени сравниваются с лицами нарушителей, находящихся в розыске. Систему можно использовать и в борьбе с банковским мошенничеством. Биометрические технологии практически исключают возможность получить кредит по подложному паспорту и снять в банкомате деньги, даже если злоумышленник знает pin-код карты.

Распознавание работает *в системах контроля доступа*. Обычно технология действует в связке с электронными пропусками: образец фото на них сравнивается с моделью, полученной в результате съемки человека, входящего в здание. В этом случае фиксация лица — самый удобный способ идентификации. Получение качественного отпечатка пальца занимает сравнительно много времени, да и не все готовы приложить палец к экрану, к которому до них прикасались десятки человек. Анализ сетчатки глаза — тоже не самая быстрая процедура: вам нужно встать точно напротив сканера и какое-то время не моргать. Лицо же всегда доступно для съемки, если только вы не носите паранджу. Фотографирование происходит мгновенно, и процедура не требует от человека никаких дополнительных действий.

Следующим вызовом для «Вокорда» в течение ближайших пяти-десяти лет станет разработка системы *по распознаванию человеческих эмоций*. Система распознавания эмоций, основанная на работе нейронных сетей, может в разы упростить и ускорить этот процесс.

Каждая из российских компаний старается захватить лидерство в разных нишах. Если заказчики «Вокорда» озабочены в первую очередь **распознаванием**

лиц в местах **массового скопления людей**, то другой разработчик, компания VisionLabs, нацелен преимущественно **на банковскую сферу**.

VisionLabs предлагает две версии системы распознавания лиц. VisionLabs Luna — платформа, которую клиенты приобретают и используют у себя. Второй продукт — облачная версия Face Is, которая доступна при оформлении подписки. Обе системы работают со сложными алгоритмами компьютерного зрения, которые выявляют специфические черты каждого лица (например, разрез глаз, форму носа и т.д.) и впоследствии позволяют найти их же на фото в архивах клиента. Luna обычно покупают крупные заказчики, в том числе банки, чтобы бороться с мошенниками, увеличивать лояльность посетителей отделений, а также следить за работой сотрудников на точках. A Face Is как более дешевый вариант покупают небольшие магазины: система, распознав лицо, находит нужную «карточку» посетителя в CRM-системе, узнает из нее его историю покупок, интересы и данные профиля.

Новую волну популярности, а также новых клиентов NTechLab принес сервис FindFace для поиска людей по фотографиям в «ВКонтакте». Сервис предлагает 30 бесплатных поисков ежемесячно; чтобы использовать его чаще и получить дополнительные настройки, нужно купить платную подписку. Большинство обычных пользователей познакомились с технологией распознавания лиц именно благодаря FindFace.

Правоохранительные органы уже используют *технологию приложения FindFace*, позволяющего связать фотографию человека, сделанную на улице, с его профилем в социальных сетях, для поиска преступников и нарушителей.

В мае 2016 г. создатель технологии *Артем Кухаренко* (N-TechLab) договорился с правительством Москвы о тестировании технологии распознавания лиц на видео, которое снимают городские камеры. Их в столице очень много: 98 тыс. на подъездах, 20 тыс. во дворах.

Людей, которые проходят мимо камер, сверяют с загруженной в систему базой преступников или пропавших людей. Если на человеке показывается высокая степень сходства, то предупреждение об этом отсылается сотруднику полиции, который находится рядом.

Алгоритм также сможет «выделять отдельных людей в любой части города и находить их страницы в социальных сетях, из которых почти всегда можно узнать многое об их жизни», искать участников протестных митингов. Даже если человек забыл телефон дома, его перемещения по городу можно будет отследить, если он попадет в объективы камер, и связать с профилем в «ВКонтакте». В полиции используют технологию для раскрытия преступлений: берут фотографии, прогоняют через приложение, находят профили людей, видят, что те вчера были онлайн, делают запрос в «ВКонтакте», там выдают IP-адрес, откуда человек выходил в соцсеть.

Нейронная сеть дает набор признаков, по которому можно отличить одного человека от другого (цвет и форма глаз, мимика и др.). Но большинство

признаков, которые выдает нейронная сеть, невидимы человеческому глазу. Точность определения изображения нейронной сетью составляет около 90%, а человеком — 25% (при объеме базы, например, в десять тысяч фотографий).

Алгоритм NTechLab дает возможность сравнивать пары лиц с 99%-ной степенью точности и проводить поиск по достаточно большой базе фотографий менее чем за 0,3 секунды с точностью более 70%. Эта технология была признана лучшей на мировом чемпионате The MegaFace Challenge, организованном Университетом Вашингтона в 2015 г. В этом чемпионате приняли участие более ста команд со всего мира, в том числе и команда Google.

Для поиска человека по базе из одного миллиарда фото такому алгоритму потребуется меньше секунды. Подобная скорость поиска может решить множество задач не только в масштабах города, а страны и даже мира. Например, поиск преступника в режиме реального времени. Среди преимуществ, помимо скорости глобального поиска по базам фотографий, у алгоритма очень высокая точность распознавания. Это стало возможным благодаря глубинному обучению и правильно подобранной архитектуре нейронной сети.

Процесс распознавания представляет собой построение вектора признаков с помощью обученной нейронной сети. Вектор признаков состоит из 80 чисел, которые содержат всю информацию о лице. Для одного человека числа похожи, для двух разных людей — отличаются. На этом отличии и построена система поиска. Важно, что информация о лице не изменится, если человек наденет очки, отрастит бороду и усы или если между фотографиями разница в несколько лет.

Стоит отметить, что информация об одном лице занимает менее килобайта на каждое изображение, что позволяет осуществлять работу алгоритма, не используя больших вычислительных мощностей.

Алгоритм достаточно устойчив к изменениям во внешнем облике и способен идентифицировать людей, если они наденут очки, отрастят бороду или сменят прическу. Узнать человека можно даже в медицинской маске, но при этом процент точности будет ниже.

В процессе обучения нейронная сеть сама формирует признаки и выбирает их в зависимости от статистических закономерностей в данных. Человеком они обычно не интерпретируются.

Для проекта с социальной сетью «ВКонтакте» было проиндексировано более *250 млн фотографий*.

Алгоритм распознавания лиц может широко применяться в различных областях, таких как розничная торговля, банковское обслуживание, обеспечение безопасности, индустрия развлечений, спортивные мероприятия, сервисы знакомств и многих др., а также для распознавания лиц преступников на видео с камер слежения или на фотографиях в социальных сетях.

На базе алгоритма NTechLab уже запущен сервис поиска людей по фото в соцсети «ВКонтакте» FindFace, который за первые три месяца набрал более

миллиона пользователей. Сервис был запущен 18 февраля 2016 г. в качестве демонстратора технологии. На сегодняшний день запущено два продукта для бизнеса — это облачный сервис FindFace Cloud API и решение FindFace Enterprise Server SDK. Теперь любая компания в мире может интегрировать технологию распознавания лиц NTechLab в свою деятельность. Сервисы предлагают два основных сценария работы: верификацию (сравнение пар лиц) и идентификацию (поиск лиц) по собственным базам фотографий любого масштаба.

Нейросети можно обучить под абсолютно разные задачи: распознавание изображений, речи, письма, предметов, эмоций и др. Этими вопросами занимаются многие мировые корпорации, такие как Google, Facebook и др. Распознавание лиц является одной из самых сложных задач.

Что ждет технологии 3D-распознавания лиц в России и в мире? С распространением автоматизации бизнес-процессов они получат все более широкое внедрение. Уровень качества технологий уже довольно высок (точность распознавания сейчас превышает 95%), а экономия времени и ресурсов огромна. Чуть больше 10 лет назад фотографии предполагаемых преступников или банковских мошенников сравнивали с имеющейся базой изображений вручную, и после 30-й фотографии человек начинает работать медленнее и ошибаться гораздо чаще. Сегодня все системы распознавания лиц не просто автоматизированы, а используют искусственные нейронные сети. Это позволяет им работать с колоссальным объемом данных, сокращать количество ошибок и увеличивать скорость.

Технологии уйдут дальше, чем исключительно **чтение лиц**. Для авторизации личности зачастую уже используется **распознавание полного образа** и, например, особенностей походки. Называется несколько сфер, куда системы распознавания лиц только приходят,— все более продвинутые рекламные технологии на стыке онлайна и офлайна или автономные автомобили, где повышенный спрос на технологии цифрового зрения объясняется их важностью для безопасности дорожного движения.

В связи с распространением технологии распознавания лиц можно было ожидать, что в скором времени появятся недорогие **контрсредства**, препятствующие такому распознаванию. Оказалось, что простым решением этой проблемы могут служить солнцезащитные очки и защитные очки Reflectacles, разработанные для защиты пользователей от распознавания по чертам лица, осуществляемого видеокамерами систем безопасности с помощью программного обеспечения, и оберегающие их частную жизнь от вторжения без их ведома.

Reflectacles — так называются светоотражающие защитные очки, разработанные Скоттом Урбаном. Урбан использовал для создания Reflectacles самые современные светоотражающие материалы.

Стоит отметить, что новинка подходит не только для велосипедистов, увеличивая их шансы быть замеченными водителями на дорогах, но и для пешеходов.

Разработано несколько вариантов очков из высококачественного светоотражающего материала.

Например, модель Reflectacles Ghost обладает способностью отражать свет видимой и инфракрасной области спектра. Это означает, что камеры видеонаблюдения, которые в основном работают с использованием инфракрасных технологий, никогда не смогут зафиксировать черты лица пользователя, если на нем эти очки. Поэтому их по праву можно назвать средством противодействия технологии распознавания лиц.

Очки Reflectacles Originals, способные отражать только видимый свет, представлены в семи различных цветовых решениях. Модели каждого из цветов имеют специфическую отражательную способность, возрастающую в таком порядке: серебряный, неоновый, золотой, синий, зеленый, оранжевый, красный.

В светоотражающих очках не используются батареи или лампочки; они просто отражают свет в направлении его источника. При облучении оправа ярко светится, не мешая пользователю.

Защитные очки собираются из цельных деталей, выполненных из прозрачного ацетата целлюлозы и подвергшихся обработке на станке с ЧПУ, вместо использования традиционной отливки из пластика в пресс-формах. В дужку очков вмонтирована металлическая проволока, повышающая прочность конструкции и дающая ультрафиолетовое излучение с помощью покрытия из высококачественного пластика CR39. Имеется возможность заменять эти стекла другими в соответствии с указанием врача.

Компания IDX и разработчик «Центр речевых технологий» в 2017 г. вывели на российский рынок сервис **удаленной биометрической идентификации личности — по лицу и голосу**. Партнеры рассчитывают, в частности, на принятие законопроекта, разрешающего такой способ идентификации для открытия счетов и выдачи кредитов в банках. К 2019 г. объем этого рынка в России может вырасти до 325 млн. долларов.

IDX добавила технологию аутентификации по лицу и голосу от компании «Центр речевых технологий» (входит в группу Газпромбанка) в свою систему управления идентификацией. Таким образом, компании-участники IDX смогут удостоверять клиентов не только с использованием документов, но и с помощью биометрических данных. Для этого достаточно, чтобы человек один раз создал и сохранил с помощью **специального приложения «цифровые слепки» голоса и лица** в информационной системе (принадлежащей, например, банку, оператору связи, страховой компании, авиакомпании). С согласия клиента такие биометрические данные могут быть использованы для удаленного удостоверения личности всеми участниками рынка без нарушения цифрового суверенитета субъекта персональных данных.

Идентификация с использованием биометрии может занять более 50% рынка идентификации в кредитных организациях в течение ближайших пяти лет.

Проведение удаленной идентификации — *обязательное требование «антиотмывочного» законодательства*, сейчас предусматривающего только два способа: через подтвержденную учетную запись клиента на портале госуслуг и подтверждаемый особым способом набор персональных данных (Ф. И. О., паспорт и т.д.).

Биометрическая идентификация набирает обороты. На рынке недвижимости есть риск столкнуться с недобросовестным посредником и стать жертвой обмана. Удаленная идентификация может быть востребована в сегментах бизнеса, где критически важно точно знать, что на другом конце находится нужный человек: например, при создании штата удаленных сотрудников, работающих с конфиденциальными данными в финансовом или юридическом секторе.

Дроны для поиска пропавших людей и против браконьеров, террористов и контрабандистов

Одними из первых, кто начал использовать беспилотники для охраны правопорядка, стали полицейские США. Федеральное управление гражданской авиации (FAA) авторизовало уже более 74 правительственных агентств по использованию беспилотников в воздушном пространстве страны, 17 из которых — правоохранительные. Наиболее известные среди них — Montgomery County в Texace, Mesa County Sheriff's Department в Колорадо и Grand Forks в Северной Дакоте.

Разрешение FAA позволило силовикам абсолютно легально задействовать беспилотники для детального обследования мест преступления и поиска пострадавших людей. Однако американские полицейские активно привлекали вышеуказанные агентства к работе и раньше, до получения последними необходимых юридических прав. Известно, что с 2013 г. группа Grand Forks успела обработать около 30 запросов силовых структур, среди которых числится 4 случая сбора данных об обстоятельствах самоубийств. С помощью дронов даже было обнаружено тело пропавшего охотника.

М. Гудман в своей книге «Будущее преступности» приводит такой пример: в 2013–2014 гг. на 80% сократился браконьерский отстрел слонов и носорогов в Африке. Секрет был прост. Американское правительство и корпорация Google в порядке гуманитарной помощи африканским странам, особо страдающим от браконьерства, предоставили подразделение патрульных и боевых дронов и обучили местный обслуживающий персонал обращению с этим грозным оружием. Единственной модификацией боевых дронов, используемых против браконьеров, было то, что с них были сняты огневые установки и встроены липучие сети и поражающие дротики со снотворным.

Полицейские США пытаются использовать дроны и в более сложных операциях, таких как наблюдение за потенциально опасными преступниками.

В июне 2018 г. компания Axon объявила, что вместе с DJI будет продавать полиции США патрульных дронов по программе Axon Air. Все дроны соединены

с evidence.com — «облачной» системой управления данными, куда будут поступать вся информация с камер дрона.

Axon Air уже предлагает свои услуги подразделениям полиции и даже перечисляет те функции, которые будут выполнять дроны: искать и спасать, осуществлять реконструкцию автомобильных аварий, наблюдать за крупными скоплениями людей, осуществлять погони и мониторинг зданий, реагировать на естественные катастрофы, анализировать места преступлений.

Дроны не слишком дороги, полностью автоматизированы и способны значительно расширить возможности полицейского контроля и наблюдения.

Беспилотники могут быть весьма эффективным поисково-спасательным инструментом для пропавших людей, но не в густых лесах, где древесный покров может блокировать сигналы GPS. К счастью, MIT придумал умное решение: использовать ту же технологию, которая управляет автономными автомобилями. Ученые разработали беспилотники, которые используют LIDAR для составления карты лесов без применения GPS. Каждый дрон создает двухмерную карту, которая включает положение деревьев, что значительно упрощает запоминание мест, которые робот уже посетил в ходе поиска.

Это, в свою очередь, позволит также совмещать карты со всего флота беспилотников и прочесывать большие участки леса с минимальными затратами усилий.

Такие беспилотники также будут более эффективными и с точки зрения способа поиска. Вместо того чтобы посылать дроны исследовать неизведанные области, метод MIT сохраняет импульс дрона как можно больше. Обычно это приводит к созданию спирального паттерна, который покрывает область гораздо быстрее. Это очень важно для спасательной миссии, когда каждая минута на счету.

Британские полицейские начали использовать практически бесшумные мультикоптеры Black Hawk, позволяющие вести видеозапись со звуком.

Также стало известно о планах британской полиции использовать беспилотники в операциях по преследованию преступников. По различным оценкам, это обойдется силовикам намного дешевле и безопаснее, чем применение мотоциклов, машин и вертолетов. Покупка дрона и его длительная эксплуатация обойдутся в сумму, меньшую, чем одна погоня с использованием вертолета (что к тому же возможно далеко не всегда) и двух полицейских машин. Вдобавок к этому применение беспилотников никак не угрожает жизни полицейских.

О первой успешной эксплуатации квадрокоптера британской полицией стало известно еще в феврале 2010 г., когда с помощью аппарата AirRobot AR100B, оснащенного системой видеонаблюдения и тепловизионной камерой, силовики графства Мерсисайд, на западе Англии, смогли разыскать в густом тумане автомобильного вора. Подобные дроны применяются в Великобритании до сих пор. Известно, что технология аппарата первоначально разрабатывалась для нужд военной разведки. Он практически бесшумный и может работать ночью, передавая изображение в режиме реального времени.

В 2016 г. рабочая группа при Совете руководителей национальной полиции и Центр прикладной науки и технологий обсуждали возможность использования беспилотных летательных аппаратов для преследования подозреваемых, использующих двух- и четырехколесные транспортные средства при совершении преступлений, говорится в заявлении Службы столичной полиции Лондона.

В последнее время лондонские полицейские борются с ростом краж, совершенных грабителями на мопедах и мотоциклах. За 12 месяцев в британской столице подобным образом было украдено более 3000 телефонов. В то же время Служба столичной полиции была вынуждена пересмотреть свою тактику преследований после инцидента, повлекшего за собой гибель 18-летнего Генри Хикса. Молодой человек погиб в погоне на высокой скорости, пытаясь на мопеде уйти от двух патрульных машин. Использование дрона может снизить шансы повторения подобного инцидента.

В конце 2015 г. дроны поступили на службу токийской полиции. Они вошли в специальный отряд по борьбе с другими дронами.

В настоящий момент беспилотники используются в правоохранительных органах целого ряда стран. Однако стоит отметить, что пока полицейские лишь оценивают потенциальные возможности подобных аппаратов. Так, в апреле прошлого года мэрия города Дубай запустила в небо дрона-полицейского, основной задачей которого стало слежение за экологическим порядком в местах отдыха и пустыне, а именно обнаружение тех, кто бросает мусор мимо урн.

Подобные дроны-полицейские смогут быстро появляться в различных местах, снимая на камеру всех нарушителей. При этом особо отмечается, что, если дроны хорошо себя зарекомендуют, силовики ОАЭ всерьез задумаются об использовании этих аппаратов для более сложных задач.

Во Франции и Японии беспилотники активно используются для дистанционного наблюдения за скоплениями людей. Однако особый интерес вызывают отдельные подразделения, которые создаются в этих странах с целью борьбы со случаями несанкционированного использования дронов. В частности, полиция Токио совсем недавно заявила, что квадрокоптеры, нарушающие те или иные правила полетов, будут отлавливаться с помощью специальных дронов большого размера. Принцип работы здесь предельно прост: к большому квадрокоптеру снизу прикрепляется сеть размером примерно 2×3 м. Далее такой аппарат догоняет мелких дронов-нарушителей и, поймав их сетью, выносит из запретной зоны.

Впервые на практике подобный метод отлавливания дронов-нарушителей был опробован в феврале 2016 г. С этого момента дроны-отлавливатели исправно несут службу в рядах силовиков. Как сообщает полиция Токио, основная цель подобных работ — защита важных локаций «с учетом самых худших возможных сценариев», из чего можно сделать вывод, что речь здесь, вероятно, идет не столько об обезвреживании дронов-папарацци, ведущих наблюдение за частной жизнью знаменитостей, сколько о противодействии серьезной

угрозе со стороны дронов-террористов, вооруженных взрывчаткой. В современном мире эта идея весьма актуальная, особенно если учесть, что, по сообщению Министерства обороны РФ, уже известны случаи использования беспилотников, начиненных взрывчаткой, в Сирии. Также летом 2016 г. ФСБ предупреждала о планах террористов использовать дроны для совершения терактов в Европе.

Согласно сообщению пресс-центра МВД, в России беспилотники различных типов стали использоваться полицейскими начиная с Олимпийских игр — 2014 в Сочи. Дроны позволяют сотрудникам правопорядка эффективнее контролировать дорожную обстановку, проводить воздушную разведку, бороться с браконьерами и т.д. Ранее стало известно, что в июне 2016 г. дроны помогли сотрудникам авиационного отряда МВД по Республике Адыгея за полгода выявить более 150 нарушений ПДД. А в Красногвардейском и Майкопском районах беспилотники позволили обнаружить нарушения в сфере недропользования и незаконные вырубки лесов.

Серьезных правовых проблем с использованием беспилотников в рядах силовиков в нашей стране нет. Однако стоит отметить, что даже этот факт не приводит к активному распространению дронов-полицейских в России — стражи порядка пока лишь присматриваются к возможности использования подобных аппаратов. При этом, по словам представителей МВД, потенциальные возможности использования квадрокоптеров велики: они могут применяться полицейскими в различных ситуациях, вплоть до обезвреживания опасных преступников.

Израильская компания Laser Detect Systems (LDS) представила на выставке HLS&Cyber Expo в Тель-Авиве первый в мире *беспилотник SpectroDrone, оснащенный датчиками для определения взрывчатки и самодельных взрывных устройств с безопасного расстояния*.

Беспилотник использует разработанную компанией лазерную систему обнаружения взрывчатки и других опасных материалов в газах, жидкостях, порошках с расстояния в несколько километров. SpectroDrone способен выполнять эти задачи, имея оперативный радиус действия 3 км.

Предполагается, что новый аппарат можно применять для розыска баз и складов террористов, а также для обнаружения мин и фугасов в зонах локальных конфликтов. В настоящее время для этих целей используют системы обнаружения взрывчатки, размещаемые на автомобильной технике, а также носимые комплекты и служебных собак.

В стране, помимо беспилотников, планируется использовать инфракрасные камеры для поимки преступников и определения людей с холодным и огнестрельным оружием.

Мэр индонезийского Макасара заявил, что с 2017 г. преступников в городе будут ловить дроны. Город планирует запустить дроны, которые будут преследовать нарушителей во время погонь. Также аппараты будут оснащены *системой*

распознавания лиц, чтобы иметь возможность определять в толпе людей, находящихся в розыске.

Макасар уже собирает различные биометрические данные своих жителей. Среди этих данных: лица, отпечатки пальцев и сканы радужки глаза. «У нас есть биометрические данные всех наших жителей — 1,8 млн. человек»,— сказал мэр города.

Мэр назвал общественную безопасность приоритетным направлением своей деятельности на весь 2017 г. Он рассказал, что, помимо дронов, некоторые улицы оснастят *инфракрасными камерами, чтобы определить людей с холодным и огнестрельным оружием.* В городе 80% преступлений совершают мотоциклисты, поэтому тепловые камеры направлены в первую очередь на них, так как определить оружие в автомобиле им не удастся.

Перспективным для полиции является *компактный квадрокоптер Snipe («Бекас»)* производства компании Aero Vironment. Он проектировался в качестве дополнительного источника информации о противнике для пехотинцев армии США и внедряется с 2016 г.

Основное предназначение наноквадрокоптера — *ведение визуальной разведки на близлежащем участке местности*. Snipe оснащен четырьмя несущими винтами и весит всего 140 гр. До момента применения дрон хранится в небольшом легком и прочном футляре.

Находясь в воздухе, Snipe производит видеосъемку *с помощью оптической и инфракрасной камер в режиме реального времени с высоким разрешением, в том числе и в темное время суток*. Мобильность камер обеспечивается встроенным механизмом поворота. Полученная картинка отображается на блоке управления оператора.

На борту беспилотника находится радиоаппаратура — встроенное УВЧ-радио и программно-определяемая радиосистема SDR,— что делает его доступным для широкого круга покупателей.

Крошечный квадрокоптер, несмотря на свои габариты, уверенно чувствует себя при порывах ветра до 24 км/ч, не создает лишнего шума, что позволяет ему оставаться невидимым для противника даже с близкого расстояния. В случае потери радиосвязи Snipe автоматически возвращается к оператору.

Американский производитель нелетального оружия Taser International заявил, что готов предоставить полиции США *беспилотники, оснащенные электрошокерами*. Компания провела переговоры с представителями полиции на конференции в Сан-Диего, пишет The Wall Street Journal.

Летом 2015 г. полиция США впервые в истории использовала робота для нейтрализации преступника. С помощью робота Remotec F-5, снабженного взрывчаткой, полицейские Далласа убили Мику Ксавьера Джонсона, застрелившего пятерых полицейских во время уличной акции. «После этого инцидента к нам поступали вопросы, возможно ли оборудовать оружием Taser автономное транспортное средство»,— говорит спикер Taser International Стив Таттл. Тазер — электрошоковое

оружие нелетального действия с радиусом действия до 10 м, позволяющее проводить задержание правонарушителя с минимумом увечий.

В полиции США считают, что применение вооруженных тазером дронов может сохранить жизни сотрудников полиции во время опасных операций, однако признают, что этот вопрос остается дискуссионным. «Неприятие обществом идеи, что беспилотные летательные аппараты могут быть оборудованы каким-то видом оружия — это препятствие, которое предстоит преодолеть»,— говорит представитель департамента полиции Портленда Пит Симпсон.

В исследовательской группе Police Foundation добавили, что такие технологии могут быть эффективным средством борьбы с преступностью, однако опасения правозащитников по этому поводу вполне обоснованы. «Многие люди обеспокоены тем, что, если вы можете вооружить беспилотник электрошокером, ничто не помешает вам оборудовать его огнестрельным оружием»,— говорит президент организации Джим Буерман.

Вооруженные дроны могут стать по-настоящему грозной силой против преступников, и для этого в некоторых странах уже прорабатывается законодательная база. Например, законодательные органы Северной Дакоты (США) еще в августе 2015 г. разрешили силовикам использовать на беспилотниках любое оружие, кроме огнестрельного. Иными словами, полицейские этого штата получили возможность дополнить дроны стреляющими электрошокерами, мощными распылителями газа и травматическим оружием, стреляющим резиновыми пулями.

В настоящий момент активно ведутся эксперименты по оснащению полицейских дронов газовыми баллончиками. Более того, французская компания Drone Volt серийно выпускает беспилотник TEAR GAS, который предназначен для распыления газа или перечного экстракта. Однако о практическом использовании такой функции дронов ничего не известно — французские силовики пока применяют эти аппараты лишь для дистанционного наблюдения за скоплениями людей.

Необходимо отметить, что потенциал использования беспилотников в рядах правоохранителей может быть ограничен не столько технически, сколько юридически. Так, американский союз защиты гражданских свобод ACLU уже выразил опасение, что вооружение полицейских беспилотников может стать причиной необоснованного применения оружия, поскольку оператор дрона не присутствует на месте событий лично, а значит не сможет адекватно ориентироваться в обстановке. Также в настоящий момент активно ведутся дискуссии с гражданскими правозащитными организациями по поводу законности использования дронов для наблюдения за подозреваемыми. Является ли наблюдение за потенциальными преступниками вторжением в их частную жизнь и есть ли в подобных случаях какие-либо исключения?

Правоохранителям и законодательным органам различных стран еще предстоит решить юридические вопросы, связанные с использованием дронов. Однако уже сейчас очевидно, что возможности силовиков с привлечением

беспилотников возрастут многократно. На сегодняшний день можно выделить следующие варианты использования дронов силовыми структурами:

- профилактическое видеонаблюдение,
- контроль массовых мероприятий,
- обеспечение VIP-встреч, включая встречи на высшем уровне,
- предотвращение террористических актов,
- контроль акций протеста,
- операции по борьбе с организованной преступностью,
- операции по поимке преступников,
- розыск пропавших людей,
- изучение места преступления,
- поддержка оперативной связи,
- предотвращение нелегальной иммиграции,
- наблюдение за наземными и морскими линиями регулярных сообщений,
- наблюдение за транспортными потоками,
- анализ причин ДТП,
- отслеживание угнанных автомобилей,
- борьба с морскими пиратами,
- предотвращение незаконной разработки недр и т.д.

Роботы-полицейские стали явью

В Аналитическом исследовании «Мировой рынок робототехники», подготовленном в 2016 г. Национальной ассоциацией участников рынка роботов (НАУРР), приводятся следующие данные.

В промышленной робототехнике с 2010 по 2014 гг. средний рост продаж в мире за год составлял 17%. В 2014 г. было продано 229 тыс. робототехнических комплексов для использования в промышленности, и 70% мировых продаж пришлось на 5 стран: Китай, Япония, США, Республика Корея и Германия. Данные страны имеют ряд государственных программ, направленных на поддержку и развитие робототехнической отрасли. Наибольшие продажи промышленных роботов в 2014 г. наблюдались в автомобилестроении (98 тыс. единиц) и в производстве электроники (48,4 тыс. единиц).

Сервисные роботы подразделяются по использованию на профессиональных и персональных. Рост продаж сервисных роботов для профессионального использования составил 11,5%, достигнув 24207 робототехнических единиц в 2014 г. Долю в 45% от данного числа занимают роботы специального и военного назначения (11 тыс. единиц). В 2014 г. было продано 4,6 млн. сервисных роботов для персонального использования, что свидетельствует о росте в 28%. Объем продаж возрос до 2,2 млрд. долларов.

Во всем мире, по данным The Robot Report, существует более 343 компаний, производящих промышленных роботов; более 347 компаний, занимающихся

интеграцией робототехнических комплексов в производственный процесс; более 886 компаний, производящих сервисных роботов для профессионального использования; 204 компании, производящие сервисных роботов для персонального использования.

Анализ тематик 100 наиболее цитируемых научных публикаций в области робототехники показал, что существует два ярко выраженных тематических кластера: базовые технологии робототехники и робототехника в медицине.

Ключевыми технологиями робототехники и направлениями перспективных исследований и разработок являются: получение энергии из внешней среды; роботы, способные менять форму и производить саморемонт; мультимодальные интерфейсы; анализ и синтез жестов; «роевой» интеллект; гибкие производственные модули и др.

По данным IFR, прогнозируется значительный рост всех сегментов рынка робототехники: продажи промышленных роботов уже в 2018 г. составили 400 тыс. единиц, продажи сервисных роботов для профессионального использования за период 2015–2018 гг. составили 152375 единиц (19,6 млрд. долларов), а продажи сервисных роботов для персонального использования — 35 млн. единиц (12,2 млрд. долларов). Myria Research считает, что общий объем рынка робототехники и интеллектуальных операционных систем, а также их экосистема, включая аппаратное, программное обеспечение и сферу обслуживания, достигнут уровня в более чем 320 млрд. долларов к 2020 г. В исследовании Myria Research общий объем рынка робототехники и интеллектуальных операционных систем в 2015 г. оценивается в 63 млрд. долларов, а в 2025 г.— 1,2 трлн. долларов. Аналитики Myria Research считают, что в течение 10 лет появится новая должность — начальник робототехнического отдела (как сейчас ИТ-директор), в связи с широким распространением использования робототехники в компаниях и важностью данных технологий для оптимизации процессов, протекающих в организациях. Myria Research дает рекомендации по оценке потенциала использования робототехники для компаний — потребителей робототехники и для поставщиков робототехнических решений. PwC считает, что с распространением роботов появится «смешанная» рабочая сила, которую будут составлять тесно взаимодействующие люди и роботы.

Что касается робототехники в России, то здесь ситуация выглядит иначе. В 2014 г. произошел значительный спад продаж промышленных роботов до 340 единиц, в то время как в 2013 г. предприятиями было приобретено 615 промышленных роботов. Доля российского рынка промышленных роботов составляет 0,15%.

Проведенный Ассоциацией опрос выявил специфику российского рынка робототехники. Как наиболее перспективную область применения промышленной робототехники респонденты отметили военную промышленность. Автомобильная и электронная промышленности, лидеры по применению промышленных роботов, не были отмечены респондентами как перспективные,

что свидетельствует об ориентации российских компаний на нужды военно-промышленного комплекса, а не на гражданский сектор. Как наиболее перспективную область сервисной робототехники респонденты назвали медицину, а также автономные транспортные средства и использование роботов для безопасности/охраны. При ответах на вопрос об ограничениях, препятствующих развитию робототехники в России, в качестве главных причин почти все респонденты выделили отсутствие квалифицированных специалистов в области робототехники и слабость образовательной инфраструктуры (устаревшие образовательные программы, слабая учебная инфраструктура и т.п.). Среди других важных причин были названы: отсутствие собственных технологических решений, непонимание ситуации на международном и российском рынках робототехники, непонимание спроса на робототехническую продукцию, недостаточность финансирования, небольшой объем рынка венчурных инвестиций внутри РФ, затрудненность экспорта/импорта технологических продуктов и их комплектующих, отсутствие понятных и прозрачных механизмов финансирования исследований, бюрократические препоны и др.

В начале 2016 г. *стартап Knightscope из Пало-Альто (Калифорния)* разработал флотилию роботов, цель которой — обеспечение общественной безопасности.

Робот Knightscope K5 может видеть, слышать, ощущать и фиксировать запахи и использует этот набор возможностей для борьбы с преступностью. По задумке разработчиков, некоторых преступников отпугнет даже присутствие робота.

Высота роботов достигает порядка 1,5 м, вес — около 136 кг. Для их передвижения используется технология, схожая с той, которая применяется в беспилотных автомобилях Google. K5 получает информацию с ряда сенсоров, анализирует ее и сопоставляет с законами и прочими данными, на основе которых может выявить факт какого-либо нарушения. Если робот обнаруживает подозрительную активность, он отправляет отчет уполномоченным лицам.

Машины записывают все, что происходит вокруг них, на камеры с высоким разрешением — обычные и инфракрасные. При необходимости устройства могут использовать микрофон и динамики для общения оператора с прохожими. Роботы сопоставляют ряд предзаписанных параметров, например звуков, с потенциальными преступлениями: машины способны реагировать на выстрел, разбитое стекло и т.д. Если подозревается нарушение, робот сохранит гео-тэг, сделает фотографии, передаст видеопоток. Устройство запечатлеет номера находящихся поблизости автомобилей, лица прохожих.

24 устройства были задействованы в Кремниевой долине для охраны кампусов и дата-центров. Глобальная задача компании — создать систему предотвращения преступлений, основанную на роботах. Стартапу уже удалось собрать порядка 12 млн. долларов. Конечно, о замене охранников супермаркетов или сокращении полицейских речь не идет, однако устройства могут помочь при

расследовании ряда преступлений и, возможно, предотвратить совершение преступных действий.

Еще более умный патрульный робот создан в Китае — Anbot. Его главное отличие от калифорнийского аналога в том, что он не только замечает внештатную ситуацию, но и легко может в нее вмешаться, во-первых, применив электрошоковое оружие (есть подозрение, что где-то внутри робота также спрятан резервуар и для слезоточивого газа), и во-вторых, погнавшись за нарушителем (машина разгоняется до 18 км/ч). Робот оценивает обстановку благодаря аудиодатчикам и камерам, размещенным со всех сторон. Кроме того, он способен реагировать на истошные крики жертв. Также у аппарата есть сенсорный экран, на котором можно нажать кнопку SOS и попросить об экстренной помощи. Робот весит всего 78 килограммов, зарядки аккумулятора хватает на 8 часов.

Также в Китае (Пекин) в рамках международной конференции — 2015 World Robot состоялась презентация трех боевых роботов китайского производства, предназначенных **для борьбы с терроризмом**.

Один из них выполняет функцию *химика-разведчика и сапера*. В его обязанности входит обнаружение отравляющих и взрывчатых веществ, после чего он немедленно передает информацию военнослужащим спецподразделений.

Второй робот будет заниматься **утилизацией обнаруженных боеприпасов.** Он весит всего около 12 кг и может транспортироваться на спине бойца. Основное его предназначение — помощь в индивидуальных миссиях.

В случае возникновения **«горячих» ситуаций** в дело вступит третий робот-боец. Он оснащен оружием небольшого калибра и гранатометом. Оснащенный современными прицелами робот сможет уничтожать террористов на дальней дистанции.

Разработчиком является компания из Харбина HIT Robot Group. Среди потенциальных покупателей боевых роботов значится пекинская полиция. Набор из трех машин может обойтись в 1,5 млн. юаней (235 тыс. долларов).

В начале июля 2016 г. полицейского робота впервые использовали для убийства преступника: в Далласе был подорван подозреваемый в стрельбе по полицейским.

Полиция решилась на использование робота для убийства преступника, так как тот отказался вести переговоры с правоохранительными органами. К гаражу, где скрывался стрелок, направили робота, обычно используемого для обезвреживания взрывных устройств. Робот не предназначен для убийства, но может переносить небольшое количество взрывчатки, потому что при необходимости подрывает большие подозрительные предметы. В этот раз к нему прикрепили примерно 450 граммов пластичного взрывчатого вещества военного назначения С-4. Этого хватило, чтобы при детонации на небольшом расстоянии от преступника нанести ему травмы, несовместимые с жизнью. Сам робот практически не пострадал: была повреждена только длинная «рука», переносящая дополнительный груз.

По словам эксперта в области военных технологий и автора книги «Изменяющийся характер войны» Питера Сингера, американцы впервые использовали такую тактику лишь внутри страны, но за рубежом американские роботы уже убивали. В Ираке военные много раз использовали в качестве самостоятельного взрывного устройства недорогого робота MARCbot (он стоит около 15 тыс. долларов). В Далласе взрыв устроил более мощный робот Remotec Androx Mark V A-1, который был приобретен полицией в 2008 г. за 151 тыс. долларов. Помимо обезвреживания бомб, он может разбивать окна, распылять слезоточивый газ, перерезать провода, пилить и проделывать отверстия. Робот не самостоятелен — каждое действие контролирует человек за пультом.

Помимо Remotec Androx Mark V A-1, в американской полиции «служит» и большое количество других роботов.

Их особенности проанализировал журналист «Медузы» Владислав Воронин (см. Meduza от 14.07.2016).

Наиболее популярны роботы, **подрывающие подозрительные предметы и деактивирующие взрывные устройства**; их использование военными заметно увеличилось во время войн в Афганистане и Ираке.

Стоимость подобных роботов колеблется от 10 до 150 тыс. долларов — в зависимости от механизмов поиска взрывчатых веществ и дополнительных функций. Как правило, полиция выбирает компактные модели, чтобы они могли пролезать под машины и проникать в различные помещения. Часто роботы снабжены микрофонами и двумя-четырьмя камерами, передающими изображения в центр управления, а также мощными сенсорами, определяющими химический состав бомбы. Полиция активно использует модель PackBot 510 с детектором Fido, который «нюхает» бомбу и быстро определяет тип взрывчатки. От этого зависит выбор дальнейшей тактики — подрыв или обезвреживание на месте.

Иногда роботы помогают полиции не рисковать и действовать максимально аккуратно **при захвате заложников**. Простые модели, снабженные панорамными камерами и мощными микрофонами, позволяют оценить количество заложников и обстановку внутри здания, **вести переговоры с захватчиками, а также доставлять еду и медикаменты по требованию**.

Для этих целей используются даже роботы, которые обычно не работают «курьерами». В апреле 2015 г. аппарат, обезвреживающий бомбы, передал телефон и пиццу мужчине, который планировал совершить самоубийство и представлял угрозу для остальных, потому что держал в руке нож. Через час после получения пиццы и начала телефонного разговора с полицейскими мужчина бросил нож и сдался.

Сложные роботы-разведчики — например, BOZ 1 — могут вскрывать двери, проламывать стены и разбивать стекла, чтобы проникнуть в закрытые помещения. Еще более мощный робот Dragon Runner, разработанный компанией

QinetiQ по заказу Пентагона, умеет подниматься по лестницам, двигать механической рукой, фиксировать движения людей и «подслушивать» их разговоры на довольно большом расстоянии. Однажды в Северной Каролине такой робот пробрался к вооруженному мужчине, который заперся в своем доме и не сдался даже после пуска слезоточивого газа. Первый аппарат преступник разбил на мелкие кусочки, но затем, когда приехал второй, между мужчиной и полицией начались переговоры (через камеру и микрофон у робота).

Другой робот в 2013 г. в Альбукерке подобрался к мужчине, который забаррикадировался в своем доме и угрожал самоубийством. Аппарат при помощи манипулятора сбросил с него одеяло, чтобы убедиться, что тот не вооружен, и только после этого в дом вбежали полицейские.

Отдельный тип роботов помогает полиции **оценивать обстановку в условиях очень плохой видимости**, например, в абсолютной темноте. Перед тем, как направить наряд полиции в темную квартиру, где могут скрываться подозреваемые, нередко активируют робота Throwbot XT (длина — 36 см, вес — 0,5 кг, шум — всего 22 дБ). Благодаря специальной оптической системе он позволяет оператору, сидящему за пультом управления, четко видеть то, что недоступно человеческому взгляду. Это существенно упрощает проведение рискованных полицейских операций.

В некоторых районах Киншасы — столицы Демократической Республики Конго — **автомобильным движением управляют человекоподобные роботы** высотой более 2,5 м. Они работают как светофоры на перекрестках с особенно беспорядочным движением.

Зеленые, желтые и красные огни размещаются на спине, груди и руках роботов. На их туловищах закреплены четыре камеры наблюдения, фиксирующие нарушение ПДД и оперативно отправляющие данные в полицейский участок. Каждый робот изготовлен из алюминия и питается от солнечной батареи, стоит 21 тыс. евро.

Уже в ближайшее время в эксплуатацию попадут сразу несколько роботов, которые сильно изменят проведение полицейских операций. Например, в Германии в 2019 г. должен появиться **робот-сапер нового уровня**. Предполагается, что сотрудникам правоохранительных органов даже не придется приближаться к подозрительным предметам, оставленным на улице: машина сама просканирует вещи и создаст 3D-модель закрытой сумки. Работа аварийно-спасательных служб сведется к просмотру готовых кадров на компьютере: инженеры должны будут проанализировать полученную картинку, сделать выводы о том, есть ли там бомба, и дать роботам следующие задания в зависимости от ситуации.

В Дубае уже появились **самостоятельные роботы-полицейские**. Они следят за безопасностью на улицах, в парках и торговых центрах. Правда, все роботы безоружны, так что в экстренной ситуации не смогут вмешаться, а только

передадут информацию полиции. Роботы, наделенные искусственным интеллектом, также предоставляют справочную информацию на шести языках, умеют шутить и заботиться о детях.

На саммите ASEAN2018 в Сингапуре для патрулирования запустили автономного робота с поворотной камерой вместо головы и мигалками. Это, само собой, привлекло внимание удивленных прохожих, которые останавливались и делали селфи. Небольшой белый робот на четырех колесах высотой около полутора метров разъезжал по периметру конференц-центра, обеспечивая дополнительную безопасность на встрече мировых лидеров.

Как сообщается, этот пока еще безымянный робот с мигающими синими и красными огнями — прототип, разработанный полицией. Он может передавать 360-градусную картинку патрулируемой местности.

В ближайшие годы у полиции появятся и **специальные роботы для убийства**. В Израиле в мае 2016 г. представили модель, которая выглядит чуть крупнее игровой приставки, но без проблем имитирует известный самозарядный пистолет Glock 26 на колесиках.

И совсем из области фантастики, которая фактически стала явью,— **о киборгах**. Исследователи из Университета Вашингтона в Сент-Луисе *превращают насекомых в киборгов*, которых можно отправить куда угодно для вынюхивания взрывчатки.

Работы ведутся по заказу ВМС США. Исследователи изучают, как насекомые анализируют запахи. Обнаружено, что саранча может идентифицировать конкретные запахи, которые ее научили обнаруживать, даже при наличии посторонних запахов. Насекомые-киборги будут более эффективными, чем роботы, потому что они используют массу природных датчиков.

Даже самые передовые миниатюрные химические устройства используют всего несколько датчиков. С другой стороны, если посмотреть на антенну насекомых, то там можно увидеть несколько сотен тысяч датчиков различных типов. Для того чтобы превратить обычную саранчу в машину по поиску взрывчатки, инженеры планируют вживить в ее мозг электроды и подключиться к ее антеннам в виде усиков, а затем расшифровать электрические сигналы. Так как операторы должны получать информацию, собранную насекомыми, исследователи также разрабатывают крошечный рюкзачок, который может передавать данные. При наличии взрывчатых веществ на приемнике будет загораться красный светодиод, в то время как зеленый свет сигнализирует об отсутствии угрозы.

И наконец, инженеры планируют нанести татуировку на крылья насекомых с помощью биосовместимого шелка, способного преобразовывать свет в тепло. Лазер, который, вероятно, будет в рюкзаке, позволит оператору контролировать действия киборга. Фокусирование лазера на левом крыле обеспечит движение насекомого влево, и то же — с правым крылом. Насекомое будет функционировать так же, как дистанционно управляемый дрон.

Новые технологии прогнозирования преступного поведения

Как известно, одним из основателей антропологической теории преступности был итальянский криминалист Чезаре Ломброзо. Он считал, что преступников можно определить по особым чертам: скошенный лоб, специфическое строение ушных раковин, различные асимметрии лица и длинные руки. Чтобы доказать свою точку зрения, он провел много измерений. Поскольку Ломброзо был по образованию доктором, он сделал сотни сравнительных вскрытий мозга — умерших преступников и обычных людей.

Долгие годы теория Ломброзо и неоломброзианцев подвергалась жесточайшей критике. Дискуссии на эту тему вновь вспыхнули в 2011 г. Группа психологов из *Корнеллского университета* продемонстрировала, что люди способны отличать преступников от других людей, просто просматривая их фотографии. Как такое оказалось возможным?

Сяолинь Ву и Си Джан из *Шанхайского университета транспорта* попытались дать ответ на этот вопрос. Ученые использовали различные алгоритмы машинного зрения, чтобы изучить лица преступников и законопослушных граждан, а затем проверили, может ли машина выявить разницу.

Предлагая свою автоматизированную систему предсказания преступных наклонностей на основе снимков лиц, китайские ученые пишут, что в отличие от людей компьютерный алгоритм классификации изображений совершенно не отягощен багажом субъективности, не имеет эмоций и неточностей, связанных с прошлым опытом, расовыми, религиозными или политическими предпочтениями, с оценкой личности человека по полу, возрасту и так далее, он не утомляется и не страдает от последствий недостатка сна или пищи.

Ученые использовали четыре подхода к автоматической классификации объектов:

- метод опорных векторов;
- метод k (метод ближайших соседей);
- логистическая регрессия;
- использование сверточной нейронной сети.

Этим алгоритмам они предложили набор из 1856 фотопортретов мужчин (китайцев возрастом от 18 до 55 лет, без бороды и усов, без шрамов и татуировок, с нейтральным выражением лица), из которых 730 попадали под подозрение полиции или имеют за плечами криминальный опыт (включая 235 из них — в связи с тяжкими преступлениями). Авторы отдельно отмечают, что лица преступников были показаны на обычных фотографиях, а не снимках, сделанных для полицейских архивов.

Пройдя обучение, все четыре алгоритма продемонстрировали определенную *способность выделять лица преступников среди законопослушных граждан*. Лучше других показала себя *сверточная нейронная сеть*, точность предсказаний

которой достигла почти 90%. Более того, авторы указывают на конкретные черты, якобы свойственные криминальной личности, включая более выраженный изгиб верхней губы, меньший угол между уголками рта и кончиком носа, увеличенное расстояние между внутренними уголками глаз.

Возможная связь между внешним видом человека и сложными чертами личности, такими как честность или жестокость, интересовала людей всегда. В худшем своем изводе эти взгляды были взяты на вооружение идеологами ультраправых движений. Однако современная наука отрицает такие однозначные и грубые взаимосвязи. Разумеется, известна *корреляция между склонностью к агрессивному поведению и уровнем тестостерона*; известно и то, что тестостерон влияет на черты лица. Однако связь между лицом и агрессией уже практически исчезает.

Все это совершенно не смущает китайских ученых, которые ссылаются на психологические исследования, показавшие, что и опытные взрослые, и даже дети 3–4 лет способны неплохо «считывать» характер других людей по лицу. Неудивительно, что статья шанхайских ученых вызвала шквал критики. Если одни обозреватели обрушились на сомнительную этическую сторону работы, то другие оспаривают саму методологию исследования.

Они отмечают, что, хотя компьютерный алгоритм действительно «не отягощен багажом субъективности», от нее может страдать сама подборка лиц, на которой он обучался и проверялся. Авторы могли, сами того не осознавая, отобрать лица, удобные для такой интерпретации. Судьи могут выносить более строгие решения по отношению к людям с суровыми и жестокими чертами лица.

В работе также сказано: в отличие от эксперта или судьи у алгоритма компьютерного зрения нет эмоций, предубеждений относительно опыта, расы, религии, политических пристрастий, он не устает, ему не нужен сон или еда. Это действительно так. Но это вовсе не значит, что машины не могут быть предвзятыми. Например, Beauty.ai *позиционировался как первый международный конкурс красоты, в котором участники оценивались искусственным интеллектом*. Как выяснилось позднее, одним из критериев оценки стала этническая принадлежность и цвет кожи, за что он и подвергся резкой критике. Результаты конкурса показали, что ИИ отдавал предпочтение более светлокожим конкурсантам.

Естественно, работа китайских ученых нуждается в более серьезном обосновании и доработке. Нужно повторить эксперимент с людьми разного возраста, пола, этнических групп и увеличить количество наборов данных. Это должно помочь разрешить некоторые спорные моменты. Например, Ву и Чжан считают, что криминальные лица можно разделить на четыре подгруппы, а законопослушные только на три. Почему так происходит? И как этот алгоритм будет работать с другими группами людей? В то же время работа поднимает важные вопросы. Если результат действительно выдерживает критику, то как его объяснить? Почему у лиц преступников гораздо больше отклонений по сравнению

с остальными людьми? Как люди определяют преступников? Это врожденное или приобретенное умение?

Если ученым удастся ответить на эти вопросы, тогда, возможно, их работа даст новый виток развития антропометрии уголовного или иного характера.

Будущих преступников можно выявить по строению их мозга в детстве.

Работающий в Университете Дьюка нейрофизиолог Авшалом Каспи и его соавторы проанализировали данные по более чем 1000 жителей Новой Зеландии, которые родились в 1972–1983 гг. и в трехлетнем возрасте проходили всестороннее медицинское, психологическое и социальное обследование. Ученые выяснили и их личные истории вплоть до возраста 38 лет, в том числе данные о приводах в полицию и об обращениях к врачам.

Это позволило выделить группу из 22 процентов людей, которые создают максимальную «нагрузку» на общество: они ответственны за 36% обращений к страховщикам, 57% ночных посещений больниц, 66% получений государственных пособий, 77% оставленных детей, 78% выписанных лекарств и 81% преступлений. По замечанию Каспи и его коллег, это распределение в целом следует известному принципу Парето, согласно которому «20% усилий дают 80% результата».

Ученые обнаружили, что попадание человека в эту группу можно с высокой точностью предсказать еще в 3-летнем возрасте по результатам обследования развития нервной системы, языковых, моторных и познавательных навыков, а также особенностей характера. Несколько лет назад Каспи и его соавторы предложили обобщать результаты таких тестов в единый р-фактор — индикатор нормального развития и состояния мозга. И хотя на попадание человека в группу риска влияют также социоэкономические факторы, фактор «здоровья мозга» (так его назвали авторы статьи) может служить хорошим предсказателем будущей судьбы.

«В богатых семьях и семьях среднего класса не так много детей с плохим состоянием «здоровья мозга»,— сказал один из авторов работы,— но если они появляются, то вырастают такими же «дорогостоящими» для социума».

Стоит отметить, что предсказательная сила этого фактора не слишком велика. В частности, для трехлеток с низким уровнем «здоровья мозга» из бедных семей вероятность оказаться в группе риска всего на 19% выше, чем для их сверстников с хорошими показателями развития.

Согласно статье, опубликованной в начале 2017 г. в издании Guardian, группе неврологов из *Виргинского медико-технологического исследовательского института Карильон* удалось установить разницу в работе мозга настоящих преступников и тех, кто совершает правонарушение непреднамеренно. Для этого достаточно лишь проанализировать снимок головного мозга.

В ходе серии экспериментов ученые просканировали мозг 40 человек, каждого из которых просили пронести через воображаемую границу чемодан. Часть участников осведомили, что в чемодане лежат наркотики. Остальные не знали, что проносят через «границу», но подозревали, что делают что-то незаконное.

Кроме того, ситуация осложнялась еще и тем, что никто из испытуемых не знал, будут ли «на таможне» проводить полный досмотр, а «таможенники» случайно выбирали людей, которых этому досмотру необходимо подвергнуть. В ходе опытов специалисты под руководством Рида Монтегю провели МРТ-сканирование головного мозга всем участникам эксперимента. Как выяснилось, во время совершения преступления у тех людей, кто осознанно нарушал закон, и у тех, кто был «преступником поневоле», проявляют активность нейроны из абсолютно разных отделов головного мозга.

Как утверждают эксперты, естественно, подобное исследование требует дальнейших изысканий, а на основании данных, полученных всего от 40 человек, рано делать какие-либо выводы. Но в случае успеха подобное обследование сможет дать новый инструмент для раскрытия преступлений.

Новейшие технологии в криминалистических и оперативных исследованиях

Прежде всего интерес представляют новые технологии, используемые **в дактилоскопии**. Они направлены на расширение возможностей по выявлению папиллярных узоров на разных следовоспринимающих поверхностях, в том числе с применением различных температурных и световых режимов (освещения) и др. В частности, английскими фирмами Polyciano Foster+Freeman, SUPERfume Foster+Freeman и Natural l Foster+Freeman разработаны технологии окуривания следов флуоресцирующим реагентом, использования цианакрилата и ИК-флуоресцентного дактилоскопического порошка. Немецкой фирмой Nincha Attestor Forensics и английскими фирмами TFD-2 Foster+Freeman и Crime-Lite Imager Foster+Freeman предложены соответственно технологии выявления следов в климатических камерах в низкотемпературном режиме после обработки поверхности раствором нингидрина, высокотепловой обработки следов на бумажных носителях, а также система полуавтоматического и автоматического улучшения качества следов. Данные технологии позволяют значительно расширить имеющиеся возможности выявления папиллярных узоров на различных следовоспринимающих поверхностях, в частности на полиэтилене, коже, металле, пенопласте и т.д.

К другому, наиболее активно развивающемуся направлению, следует отнести расширение сферы использования компьютерной техники и информационных технологий — криминалистическое исследование информации из мобильных устройств: данные о входящих и исходящих звонках, контактах, полученных и отправленных сообщениях, в том числе содержащихся в закодированном или скрытом виде, и др.

Практика борьбы с преступностью свидетельствует, что, с одной стороны, научные достижения в абсолютном большинстве случаев используются преступниками для совершения преступлений, а с другой — что развитие

инновационных технологий и их активное внедрение в различные сферы общества, в том числе и в правоохранительную, включая экспертную, создает необходимые условия для интенсивного научного творчества, поднимая на новый уровень современные возможности экспертных учреждений России. Прежде всего это относится к медицинскому (биологическому), психологическому и некоторым другим направлениям, в которых наиболее хорошо разработаны инновационные подходы к решению задач выявления диагностических признаков и свойств человека.

Как известно, методы решения диагностических задач (и их достаточно много) наиболее хорошо разработаны в вышеназванных направлениях, что обусловливает повышение роли судебных экспертиз как средства выявления диагностических признаков и свойств человека.

Магнитно-резонансная томография (МРТ) как разновидность метода лучевой диагностики является наиболее перспективным направлением для получения диагностической информации при проведении судебно- медицинских исследований. Основным преимуществом применения данного метода является возможность длительного хранения объективных результатов исследования, в том числе в электронном виде. Более того, по результатам МРТ возможно установить прижизненный или посмертный характер колотых, огнестрельных и других повреждений на трупе, обнаружить гематомы (кровоизлияния), переломы костей в затруднительных при обычном вскрытии трупа местах, например в области лица, головы, внутренних органов и др.

Выполнение посмертной МРТ или компьютерной томографии (КТ) повышает диагностические возможности судебно-медицинского или патологоанатомического исследований. Благодаря проведенному исследованию возможно повысить объективность получаемой информации, в частности при определении вида, характера и давности наступления смерти, возможных изменений, патологии в организме при патологоанатомическом вскрытии трупа и т.д.

Отдельного рассмотрения заслуживает генотипоскопическая экспертиза (ДНК-идентификация), проводимая в настоящее время, как правило, по тяжким преступлениям, совершенным против личности (убийство, изнасилование и др.). Необходимость в использовании генотипоскопической экспертизы возникает и в тех случаях, когда проведение визуального опознания данной категории погибших не представляется возможным — по причине произошедших необратимых изменений внешнего облика человека.

Учет биометрических параметров человека при решении диагностических задач на первоначальном этапе предварительного расследования позволяет выделить некоторые его свойства и признаки, по которым возможно проведение оперативно-разыскных мероприятий.

В этом отношении определенный интерес представляют исследования в данной области разработчиков американской компании Advanced Optical Systems,

позволившие считывать узоры папиллярных линий человека бесконтактным способом в течение 0,1 секунды посредством устройства AIRprint. Считывание папиллярных линий осуществляется источником поляризационного света и двух камер, фиксирующих свет различной поляризации. При этом человек должен находиться в состоянии статичности (неподвижности) на расстоянии до 2 м от камер. Отражение поляризационного света от папиллярных линий и бороздок происходит по-разному: первые отражаются горизонтально, вторые — вертикально. В ходе последующей компьютерной обработки можно получить изображение только одного пальца человека. Несмотря на это, в случае если в дактилоскопической базе данных имеется его дактокарта, установить личность данного человека возможно в течение короткого промежутка времени.

Помимо этого, данные системы применяются в биометрическом контроле авиапассажиров при их биометрической регистрации перед входом в зону досмотра и посадки в самолет, а также при автоматической регистрации паспортных данных.

Многие из нас читали научно-фантастические рассказы или смотрели фантастические фильмы, в которых полицейские и детективы, добравшись до места преступления и используя специальный сканер, ищут отпечатки и ДНК убийцы и здесь же, на месте, сравнивают их со своей базой данных. Ученые из Массачусетского технологического института (MIT) смогли миниатюризировать технологию, носящую название *масс-спектроскопия.* В настоящий момент применение этой технологии возможно исключительно в специальных лабораториях, и ее сутью является *анализ различных субстанций и их определение*. Как вы уже могли понять, наличие под рукой такой технологии и возможность ее использования прямо на месте преступления могли бы оказаться очень полезными для более быстрого и эффективного расследования дела.

Специалисты MIT объясняют, что смогли уменьшить все компоненты тестового оборудования до наноскопического уровня. И теперь вместо необходимости в наличии целой специально оборудованной лаборатории для проведения нужных тестов следователи смогут использовать небольшие карманные гаджеты размером со смартфон. При этом устройство будет настолько эффективным, что сможет упаривать (выделять нужные элементы) образцы без потери качества.

Ученые из *Университета Калифорнии в Сан-Диего* смогли узнать о пищевых предпочтениях, состоянии здоровья и образе жизни добровольцев, взяв биохимические пробы с поверхности их смартфонов.

«Представьте себе сценарий, в котором следователь находит какую-то персональную вещь — к примеру ручку, телефон или ключ, на которых нет ДНК преступника, или же его ДНК нет ни в одной базе данных. И на этом расследование закончится. Мы подумали: что, если мы воспользуемся следами химии его кожи на этих предметах для определения того, какой образ жизни ведет хозяин?» — говорит автор исследования Питер Доррештайн.

Для этого ученые использовали *масс-спектрометрию* — метод исследования вещества путем идентификации и определения структуры сложных органических молекул. Они взяли несколько проб с передней и задней панели телефона, а также с четырех точек на правой руке владельца. В исследовании приняли участие 39 добровольцев.

Ученым удалось определить 500 различных молекул. Сравнив их с имеющимися образцами в базе данных, они смогли описать примерный образ жизни каждого владельца телефона. «Если владелец — женщина, мы можем определить, пользуется ли она дорогой косметикой, красит ли волосы, пьет ли кофе, предпочитает ли пиво вину, любит ли острую пищу, лечится ли от депрессии, пользуется ли солнцезащитным кремом или репеллентами от насекомых, а в связи с этим — сколько проводит времени на открытом воздухе и другую информацию. Это та информация, которая может помочь следователю сузить круг поиска владельца объекта»,— говорит соавтор исследования Амина Боуслимани из Университета Калифорнии, Сан-Диего.

Легче всего таким образом оказалось определить пищевые привычки человека: на телефонах остались молекулы цитрусовых, кофеина и алкалоидов. В основном эти молекулы переносятся на телефон через кожу рук и пот. А следы солнцезащитных средств и средств от комаров удалось обнаружить спустя несколько месяцев после последнего использования.

Тем не менее наиболее важным является не идентификация человека с помощью смартфона, которая все-таки сильно уступает по надежности тестам ДНК или проверке отпечатков пальцев, а составление его портрета по следам, обнаруженным на телефоне. По мнению ученых, подобный анализ может быть полезен как для медиков, так и для полицейских. «Вы можете сузить выборку, узнав, мужчина это или женщина; если вы обнаружите, что человек пользуется солнцезащитным кремом, вы можете выбирать среди людей, которые много времени проводят на свежем воздухе,— все эти небольшие подсказки сужают круг возможных подозреваемых при расследовании»,— заявил один из авторов исследования Питер Доррестейн из Калифорнийского университета. Также этот метод может применяться и в других случаях — например, чтобы проверить, принимает ли пациент назначенный ему препарат.

По мнению авторов исследования, может быть создана база данных, в которой будут примеры различных веществ, она поможет полиции делать выводы об образе жизни и привычках владельцев смартфонов, ключей и других найденных предметов.

По мнению Мелани Бейли, эксперта по криминалистическому анализу из Университета Суррея, такой подход может оказаться полезным. «Проблема в том, что, если вам в руки попал смартфон, вы можете получить отпечатки пальцев, но они будут бесполезными, если владельца смартфона нет в базе данных или если отпечатки смазаны. А информация, полученная таким образом,

позволит вам сузить список подозреваемых или по крайней мере понять, с человеком какого рода вы имеете дело»,— считает она.

Авторы отчета RAND Corporation за 2016 г. считают, что в этом случае в качестве свидетелей преступлений, а вернее фиксаторов информации, начинают использоваться гаджеты. Действующее законодательство пока не готово к такому повороту событий, а первые прецеденты зачастую нарушают права человека.

Органы правопорядка начнут использовать не только полученные от сотового оператора сведения о передвижениях пользователя смартфона и детализацию его звонков, но и такие физиологические детали, как сердечный ритм и степень физической активности человека. Фитнес-трекеры помогут узнать, когда и куда бежал подозреваемый. Впрочем, доступ следствия ко всей информации в личных гаджетах пока затруднен из-за пробелов в законодательстве.

Отчет приводит в пример случай со смартфоном стрелка из Сан-Бернардино, к которому полиция пыталась получить доступ при содействии Apple. Айфон убитого преступника был защищен паролем, и ФБР потребовало от компании ПО для разблокировки. Apple отказалась содействовать, но спецслужбам удалось самостоятельно получить доступ к данным. Это лишь один из наиболее громких прецедентов в ряду похожих историй.

Гаджеты станут еще более полезным инструментом для полицейских, и, как полагают авторы отчета, полиция активно начнет их использовать. Это происходит уже сегодня. Недавно полиция потребовала от Amazon предоставить аудиоданные с колонки Amazon Echo, которая находилась в комнате подозреваемого. Стражи порядка нашли и другие свидетельства против обвиняемого. В ночь убийства в доме умные счетчики воды зарегистрировали расход более 500 литров. Предполагается, что так преступник пытался отмыть следы крови и замести следы преступления.

Авторы отчета подчеркивают, что подобное использование гаджетов пока никак не обозначено в правовой системе. Более того, оно противоречит Пятой поправке к Конституции США, которая позволяет обвиняемому не свидетельствовать против себя. Подозреваемый не обязан предоставлять пароль от своего смартфона, хотя некоторые представители власти думают иначе. Отсюда возникает беспокойство, что со временем досмотр смартфона станет такой же стандартной практикой, как и досмотр автомобиля на дороге.

Полиграфы с искусственным интеллектом

Как известно, первый прибор для детекции лжи назывался *гидросфигмометр*. Его стал использовать итальянский криминалист *Чезаре Ломброзо*. В 1890-х гг. с помощью гидросфигмометра он измерял у подозреваемых давление крови в то время, пока их допрашивала полиция. Ломброзо утверждал, что может определить, когда преступники лгут. Показывая фотографии, связанные или не связанные с преступлением, он одновременно фиксировал частоту пульса и крови у подозреваемых.

Прообраз современного полиграфа разработал в 1920-х гг. *Джон Ларсон*, офицер калифорнийской полиции. Созданное им устройство фиксировало одновременную регистрацию кровяного давления, пульса и дыхания. С помощью этого аппарата было проведено большое количество проверок лиц, подозреваемых в уголовных преступлениях. Ларсон назвал свой инструмент *полиграф*, позаимствовав это название у Джона Хавкинса, придумавшего этот термин в 1804 г. Так называлась изобретенная им машина для создания точных копий рукописных текстов. Название «полиграф» произошло от двух слов — «поли» (много) и «граф» (писать). Этим аппаратом пользовались в XIX веке многие, включая Томаса Джефферсона, третьего президента США и автора Декларации независимости. Однако именно Джону Ларсону принадлежит первенство в приложении слова «полиграф» к прибору для определения лжи.

В 1926 г. ученик и сотрудник Джона Ларсона по имени Леонард Килер ввел в уже имеющийся полиграф дополнительный канал, регистрирующий изменение кожного сопротивления. Это значительно повысило точность тестирования.

За столетнее существование полиграфы получили широкое применение. В XXI веке отмечается тенденция увеличения практики применения психофизиологических экспертиз с использованием полиграфа в ведущих странах мира: США, Франция, Италия, Германия. Военная разведка, полиция, Министерство обороны, ФБР, ЦРУ применяют эту методику, так же как и промышленные компании, банки, торговые фирмы. По данным Американской ассоциации операторов полиграфа, в настоящее время полиграф используется более чем в 60 государствах.

На сегодняшний день и в России сложилась следственная и судебная практика проведения психофизиологических экспертиз с использованием полиграфа. За последние годы разработана система применения полиграфа к оперативно-разыскной деятельности: создана нормативная база; разработаны квалификационные требования к специалистам, проводящим опросы, и методика их подготовки; отработаны приемы проведения опроса и подготовлены рекомендации по его проведению.

В уголовном судопроизводстве также имеются прецеденты принятия заключения экспертов-полиграфологов судами первой инстанции в качестве доказательства. Заключения экспертов-полиграфологов в совокупности с иными доказательствами, собранными по уголовному делу, не только находят отражение в обвинительных заключениях, но и ложатся в основу судебных решений.

В известном специалистам письме Генеральной прокуратуры России (исх. № 28–15–05 от 14.02.2006 г.) «Обобщение практики использования возможностей полиграфа при расследовании преступлений» отмечается, что «в последние годы следственные и оперативные органы все чаще стали обращаться к возможностям полиграфа (детектора лжи, лай-детектора), используемого более полувека во многих странах мира. Управление криминалистики Генеральной

прокуратуры Российской Федерации на основе анализа информации из прокуратур субъектов Российской Федерации провело обобщение практики использования полиграфа при расследовании преступлений.

Обобщение показало, что полиграф стал применяться не только при осуществлении оперативно-разыскных мероприятий, но и для получения новых доказательств путем производства психофизиологических исследований в виде заключения эксперта или специалиста. Опросы в основном проводятся специалистами-полиграфологами, состоящими в штате органов внутренних дел. Экспертизы назначаются и производятся в подразделениях МВД России и в экспертных учреждениях Минюста России, а также нештатными экспертами…

…В соответствии с УПК РФ оценка доказательств производится по внутреннему убеждению участников уголовного процесса, и полиграф может сыграть определенную роль как дополнительный элемент убежденности в невиновности конкретного лица в инкриминируемом ему деянии или, наоборот, способствовать изменению ориентира в расследовании, отступлению от неверных предположений о причастности лиц к исследуемым событиям…

…Результатом подбора обоснованных и необходимых вопросов к опрашиваемому лицу может стать не только возможность получения признательных показаний, но и выявление дополнительных обстоятельств, существенно расширяющих доказательственную базу, а именно: установление вещественных доказательств, отыскание трупа…

…Трансформация результатов опроса на полиграфе как одного из видов оперативно-разыскных мероприятий в процессуальную форму для последующего использования в процессе доказывания нашла свое распространение в Брянской области, где механизм закрепления результатов опроса состоит из следующих этапов:

- *к материалам уголовного дела приобщается справка-меморандум о проведенных оперативно-разыскных мероприятиях и справка специалиста- полиграфолога;*
- *допрос специалиста о результатах опроса и научных методах, используемых при снятии данных и подсчете результатов полиграмм;*
- *допрос ранее опрошенного лица с предъявлением результатов опроса…*

…Несколько иным способом, наиболее перспективным, возможности полиграфа при установлении и доказывании обстоятельств используются работниками прокуратур Астраханской, Тамбовской и Саратовской областей, г. Москвы, а также республик Мордовия, Бурятия и Северная Осетия — Алания. Ими назначается нетрадиционный вид судебных экспертиз — психофизиологические, результаты которых в дальнейшем, при раскрытии преступлений и направлении уголовных дел в суд, используются в качестве доказательств.

В Республике Бурятия по двум уголовным делам, рассмотренным с вынесением обвинительных приговоров, заключения комплексных психолого-психофизиологических экспертиз, произведенных полиграфологом и психологом, являлись одним из доказательств…

…Эффективность использования детектора лжи в отмеченных, а также во многих других ситуациях, с которыми часто приходится сталкиваться работникам прокуратуры, безусловна. Следователь уполномочен самостоятельно направлять ход расследования и принимать решения о производстве следственных и иных процессуальных действий. При этом адекватным противодействием преступности является и совершенствование путей поиска доказательств, и придание им (дозволенными методами) трудноопоримой процессуальной значимости…»

Современные полиграфы бывают самыми необычными. Например, в 2002 г. появились принципиально новые детекторы лжи. Новая модель реагирует *на изменения температуры вокруг глаз*. Это один из первых приборов, считывающих психофизические данные без непосредственного контакта с телом человека. Более того, данные обрабатываются мгновенно и экспертиза не требует присутствия психофизиологов, как в случаях с традиционными детекторами лжи.

Принцип действия основывается на том, что, когда человек испытывает психический дискомфорт — лжет либо лукавит,— у него повышается внутриглазное давление, наблюдается прилив крови к глазным яблокам, из-за чего температура окологлазного пространства повышается.

Устройство предназначено для использования в аэропортах и на контрольно-пропускных пунктах. Оно представляет собой термокамеру, фиксирующую в инфракрасном изображении изменение температуры. Самая маленькая камера может иметь размеры почтовой марки. Изображение поступает на компьютер. Прибор безошибочно срабатывает в 80% случаев.

Открытие связи инфракрасного эффекта и эмоционального состояния произошло, как это часто бывает, случайно: ученые изучали зависимость метаболизма от физической активности. Во время серии экспериментов испытуемого, жующего жвачку, исследовали при помощи термокамеры. На снимках были отчетливо видны температурные «разводы» и перепады в лицевой части в связи с интенсивным жеванием. Внезапно на пол лаборатории упала книга, и испытуемый, испугавшись, вздрогнул. Камера зафиксировала изменение «термопортрета».

Но и этот детектор несовершенен. Внести погрешность в результат могут самые различные факторы: наличие сквозняка в помещении или пища, которую ел подозреваемый незадолго до допроса.

В конце 2000 г. был создан портативный детектор лжи Handy Truster, который *интерпретирует малейшие изменения в голосе человека*. Результат прослушивания голоса отображается на экране в виде надкушенного яблока и крышки над чайником. Яблоко характеризует волнение и лукавство: слегка надкушенное — подозрительное волнение, половинка — попытка избежать ответа, худой огрызок — ложь. Положение крышки описывает уровень стресса: на чайнике — человек спокоен, подлетела в воздух — раздражен, вскипела до предела — взбешен.

В NASA разрабатывается новая технология, которая может избавить нас от необходимости произносить слова вслух. Дело в том, что, когда человек говорит сам с собой, мозг посылает сигналы управления языком, тот непроизвольно шевелится, в то время как воздух не подается, и рот человека закрыт.

Специальные сенсоры улавливают колебания языка и считывают их, преобразуя в связную информацию. Сейчас система имеет маленький словарный запас, но уже в состоянии понять, о чем человек думает. Технологию можно использовать в сотовых телефонах и похожих устройствах.

В портативном детекторе эмоций *Truster корейского производства* технологически используется принцип того, что вне зависимости от языка (русского, английского или даже банту), когда человек обманывает, в голосе появляется «предательская дрожь». Действительно, во время высказывания учитывается тональность, громкость, а также профиль правдивых ответов. Первоначально устройство калибруется, для этого вы должны включить соответствующий режим и задать около 5–6 вопросов, ответы на которые будут заведомо правдивыми.

Диагноз-01 является универсальным компьютерным полиграфом. В организме человека было обнаружено явление, которое называют *психологической дрожью или же мускульной микродрожью*. Дрожь сама по себе проявляется виде колебаний и волнообразных движений работающих мышц. Пока человек находится в спокойном состоянии, амплитуда колебаний достигает максимального уровня и убывает пропорционально степени стресса. Голосовые связки образуют мембраны, управляют которыми три группы мышц. Они придают им такую форму, что проходящий через них воздух создает настолько высокий звук, насколько сильно напряжение мышц. Отклонения очень незначительны, и человеческий слуховой аппарат просто неспособен их уловить, чего нельзя сказать о технических средствах. Они фиксируют и обрабатывают эту микродрожь. Такой эффект проявляется в изменении параметров голоса.

Когда человек говорит неправду, у него происходит микростресс, из-за которого происходит снижение модуляции голоса. Это явление легло в основу разработки психологического **определителя стресса (PSE)**. Этот прибор был запатентован в Канаде, США, Японии и Великобритании.

Голосовой анализатор стресса обладает рядом преимуществ перед обычным детектором лжи. Поскольку исследуется прежде всего голос, то пропадает необходимость подключать к человеку датчики. Также появляется возможность использовать запись, что решает проблему личного присутствия испытуемого. Вопросы можно задавать в обычном темпе. В силу того, что тестируемый человек вынужден отвечать полными, развернутыми предложениями, исчезает неестественность.

Новый детектор лжи был разработан в Министерстве внутренних дел Великобритании. Принцип действия нового полиграфа существенно отличается от традиционных. Этот аппарат не имеет с испытуемым контактов в виде

множества датчиков. Поэтому человек может даже не догадываться о том, что его поведение и речь анализируют.

В структуру системы входит *обычная видеокамера, набор алгоритмов и тепловой датчик высокого разрешения*. Действует механизм, основываясь на неосознанном выражении человеком эмоций, на выражении лица, приливе крови к коже.

Создатели нового полиграфа оценивают его точность приблизительно в 70%. Так как эта система не гарантирует стопроцентной надежности, ее использование планируют совмещать с другими способами анализа правдивости.

Исследователи *из Мичиганского университета* нашли применение в качестве детектора лжи машинного обучения. Для проверки точности системы ученые использовали 120 видео с реальных судебных заседаний. Предметом анализа стали речь и жесты выступающих. Искусственный интеллект в 75% случаев определил, когда человек лжет, а когда говорит правду. Люди смогли выявить ложь лишь в 50% случаев. Программное обеспечение учитывало такие факторы, как направление взгляда говорящего, использование слов-паразитов и повторяющиеся жесты — движение головы, рук, бровей и рта.

По итогам исследования ученые сформулировали главные «симптомы» лжи. К ним относятся движения рук, чрезмерная мимика, использование звуков-паразитов («эээ…», «мм…» и других), попытка придать речи большую убедительность, частое кивание головой и намеренное стремление смотреть в глаза тому, кто задает вопросы.

В будущем устройства смогут давать более точную оценку, так как станут замерять сердечный ритм, дыхание и температуру тела говорящего. Для этого не понадобятся даже датчики: программа сможет делать это на расстоянии, используя технологию тепловидения.

Группа ученых *из Лондонского городского университета* разработала алгоритм для выявления лжи по структуре и особенностям языка. Программа поможет не только раскусить мелкий обман о болезни или задержке дедлайна, но и укажет на случаи мошенничества и предательства.

Ученые исследовали архив электронных писем и на его основе выявили несколько признаков лжи, которая отражается в языке на микроуровне (выбор слов, их использование), на макроуровне (структура письма) и на метауровне (взаимосвязь между частями текста). Для разработки алгоритма использовались большие данные и система распознавания естественной речи. Оказалось, что неискренность в письмах выдает отсутствие личных местоимений и использование излишних прилагательных. Также авторы таких сообщений часто излишне структурируют свои аргументы, стараются минимально осуждать самих себя и делают акцент на похвале. При этом люди зачастую подстраиваются под собеседника и меняют тон сообщения в соответствии с его тоном.

Ученые отметили, что алгоритм предназначен для того, чтобы обезопасить организации от мошенничества и финансовых потерь. Разработка может использоваться не только внутри компании, но и для анализа переписки с клиентами.

Стартап из Торонто NuraLogix запатентовал новый метод распознавания скрытых эмоций по видеозаписи. Технология под названием трансдермальное оптическое изображение позволяет определять эмоции человека на основании изменения лицевого кровотока, игнорируя мимическое выражение.

Под кожей нашего лица существует большая сеть кровеносных сосудов. Когда мы испытываем различные эмоции, наш лицевой кровоток едва заметно изменяется. И эти изменения регулируются автономной системой, которая неподвластна контролю нашего сознания. Глядя на перемену лицевого кровотока, мы можем обнаружить различные человеческие эмоции. Так как изменения кровотока невозможно увидеть невооруженным глазом, ученые разработали новую методику создания изображений, которую назвали трансдермальным оптическим изображением — Transdermal Optical Imaging (TOI). Сначала они снимают на обычную видеокамеру лицо человека, эмоции которого хотят расшифровать. Затем, используя эту технологию, извлекают трансдермальные изображения изменений лицевого кровотока. Алгоритм измеряет концентрацию гемоглобина, входящего в состав крови.

Применяя новейшие алгоритмы машинного обучения и нейронауки, можно использовать эту информацию для моделирования и обнаружения скрытых человеческих эмоций — независимо от выражения лица.

В мае 2017 г. российскими разработчиками из Новосибирска представлено приложение Verity, которое распознает ложь, считывая мимику человека, говорящего на камеру. В разработке использованы современные мобильные технологии: компьютерное зрение, машинное обучение, элементы искусственного интеллекта.

Приложение Verity — первый в мире детектор лжи в виде приложения, пользоваться которым смогут обычные люди. При этом вердикт приложения строится на максимально научных основаниях.

Самой главной задачей на первом этапе разработки стал вопрос данных, которые станут *основанием вердикта мобильного детектора лжи*.

В итоге работа приложения выглядит так:

- с помощью компьютерного зрения приложение собирает данные о мимике, пульсе и движении зрачков говорящего на камеру человека;
- далее обученный машинным способом алгоритм сравнивает полученные данные с паттернами двух типов: экспертные паттерны на основе исследований психологов и паттерны, выявленные самим алгоритмом в ходе обучения на людях;
- в результате сравнения выводится вердикт в процентном соотношении.

Приложение Verity умеет распознавать человеческое лицо. Оно считывает микродвижения и пульс с лица: программа выделяет на лбу определенный, наиболее подходящий, участок и по микроизменению тона кожи может распознать колебания

пульса. Также влияет движение глаз, бровей, губ, щек. Чтобы выяснить, говорит человек правду или нет, нужно навести на собеседника камеру и задать вопрос. Приложение запишет на видео лицо говорящего и выдаст результат в процентах.

Тестирования показали, что верные вердикты выдаются в более чем 80% случаев. Работа над улучшением алгоритма до сих пор ведется. После релиза приложений для iOS и Android начали разрабатывать версию для десктопа, которую можно использовать, например, при собеседованиях по «Скайпу».

Саратовские ученые из Лаборатории математического моделирования правовых явлений и процессов Саратовского госуниверситета им. Чернышевского изобрели и запатентовали бесконтактный дистанционный полиграф, оценивающий достоверность информации без контакта с испытуемым.

В отличие от аналогов данный аппарат не требует закрепления датчиков на теле. Достоверность информации определяется по невербальным признакам — изменению тембра и громкости голоса, темпа речи, количеству запинок и других. Заложенный в аппарат принцип решает две проблемы современных полиграфов. Во-первых, он не требует добровольного согласия испытуемого на прохождение теста. Во-вторых, работа полиграфа может проходить в удаленном доступе, например с использованием существующих средств дистанционной аудиосвязи.

Принцип работы саратовского полиграфа основан *на сложном алгоритме, который оценивает десятки невербальных признаков речи*. Новая технология уже отработана на практике: с использованием данной методики в последние годы было проведено более 150 судебных экспертиз. Все результаты были подтверждены параллельным исследованием на классическом полиграфе и оперативно-разыскными мероприятиями.

Сегодня программное обеспечение для полиграфа продолжает совершенствоваться. Конечная цель — создать такой продукт, в котором анализ показаний проводился бы в автоматическом режиме. Это значительно упростит использование полиграфа, снизит себестоимость экспертизы и требуемое время на подготовку специалистов.

В перспективе детектор лжи можно будет устанавливать в качестве приложения на обычный смартфон или планшет. Однако это не значит, что воспользоваться им сможет любой желающей. Необходимо обучение для правильного проведения интервью. В первую очередь он рассчитан на профессиональное использование и оперативно-разыскную работу.

Российская компания Tselina Data LAB, использующая для создания программного обеспечения алгоритмы машинного обучения, разработала программный алгоритм глубокого обучения для камер под названием Fraudoscope, который определяет ложь по эмоциям на лице человека. Натренированное с помощью CUDA и графических процессоров TITAN X и распознающее ложь приложение использует камеру высокого разрешения для съемки допросов и декодирования результатов. Камера направлена на допрашиваемого, и программное

обеспечение отмечает на видео изменение пикселей, которые соответствуют дыханию, пульсу, расширению зрачка, лицевым тикам. Уже сейчас незавершенное приложение демонстрирует точность более 75%.

Как и в случае с тестами на полиграфе, при использовании Fraudoscope для калибровки опрашиваемому необходимо задать вопросы, ответы на которые хорошо известны. Ему также предлагают представить, что он только что выиграл олимпийскую медаль. На примере того, как человек обдумывает вымышленные ответы, система учится распознавать ложь конкретного испытуемого.

Группой пермских ученых совместно с работниками ГУВД Пермского края предпринята попытка создания интеллектуальной программы обсчета полиграмм с использованием принципиально нового подхода, основанного на применении современных нейросетевых технологий и социальных генетических алгоритмов. Новый подход позволил бы устранить все отмеченные недостатки существующих полиграфов, уменьшить влияние человеческого фактора и, таким образом, значительно повысить точность работы полиграфа.

Принципиальное отличие нового подхода состоит в том, что разработчики применили современные методы искусственного интеллекта. Они максимально отказались от использования известных закономерностей и правил, традиционно закладываемых в обсчитывающие программы. Эти правила в неявном виде автоматически формируются самой компьютерной программой в ходе обмена информацией между прибором и обследуемым человеком. Компьютерная программа, являясь системой искусственного интеллекта, сама извлекает и формализует в виде правил закономерности организма опрашиваемого человека, автоматически настраивается на его индивидуальные физиологические особенности, отсеивает возможные артефакты. В конечном итоге сокращается объем и время работы полиграфолога, уменьшается влияние человеческого фактора, увеличивается компьютерная достоверность обсчетов.

Британские ученые из Университета Кардиффа (Уэльс) разработали и в октябре 2018 г. продемонстрировали нейросеть, которая поможет правоохранительным органам и другим силовым ведомствам разоблачать лжецов. Устройство на 80% точно *определяет ложь в письменном тексте* и в скором времени должно заменить полиграф.

Данную технологию уже используют испанские полицейские участки. Искусственный интеллект VeriPol определяет ложь с вероятностью до 91%. Система вычисляет наиболее распространенные комбинации слов, которые используются при обмане полицейских.

Заключение

Учитывая наличие гремучей преступной смеси технологий новой промышленной революции и проблем глобальной нестабильности, борьба с криминалом ближайшего будущего будет сочетать привычные методы полицейской деятельности,

традиционные криминалистические средства, новейшие достижения в использовании искусственного интеллекта, робототехники, технологий 3D, геолокационных систем, возможностей видео-, аудио- и генетической идентификации, использование детекторов лжи, работающих на совершенно новых принципах.

Причем, наращивание потенциала новейших технологий в борьбе с преступностью в чем-то будет иметь вынужденный характер, учитывая дефицит финансовых ресурсов, не позволяющий увеличивать кадровый состав правоохранительных органов и спецслужб.

Современные правовые конструкции должны быть адекватны достижениям технологической революции. Речь идет о разработке новых моделей правового регулирования, в том числе возникающих и в сфере уголовно-правовых отношений; о пересмотре в ряде случаев правового языка; о правовом допуске искусственного интеллекта для подготовки приговоров по уголовным делам.

Для интеграции в единое мировое цифровое пространство России придется синхронизировать законодательство в области цифровой экономики и цифровой безопасности с теми странами, в которых зарегистрированы крупнейшие международные цифровые корпорации.

Технологическая революция развивается небывалыми в истории темпами. В скором времени, например, будут запущены сети пятого поколения (5G), которые обеспечат работу интернета вещей, искусственного интеллекта, виртуальной и дополненной реальности, обеспечат удаленное управление автотранспортом, работу телемедицины и многое другое, в том числе работу «умной», «цифровой» полиции и «умных», «цифровых» судов. 5G — это не одна технология, а набор технологий радиодоступа, включая революционные, которые потребуют своего правового обеспечения и защиты от преступных посягательств.

Компания IBM и ее партнеры по производству чипов Globalfoundries и Samsung разработали *технологию производства транзисторов, которая приведет к появлению 5-нанометровых чипов*. Новые чипы могут уместить 30 млрд. транзисторов, хотя по размерам будут не больше ногтя (для сравнения: 7-нанометровый чип умещает 20 млрд. транзисторов).

Специалисты IBM планируют использовать технологию при создании *собственных когнитивных вычислительных систем, интернета вещей и других объектов, «связанных с переработкой больших объемов данных»*.

И это еще только начало. Сейчас индустрия работает над оптоэлектронными чипами первого поколения, в которых используются *большие фотонные волноводы*. Эти чипы, видимо, появятся на рынке через три-четыре года. А российские ученые работают над тем, чтобы сделать *второе поколение этих чипов* более компактными: это позволит увеличить количество ядер от сотни на одном кристалле (как сейчас) до тысяч, а значит, возрастет и производительность. То есть мы получим *настоящий суперкомпьютер на одном единственном маленьком полупроводниковом кристалле*.

Многие известные ученые считают, что *информационной атомной бомбой* может стать создание *квантового вычислительного устройства*, которое способно устроить для нашей цивилизации настоящую катастрофу. Практически вся информационная инфраструктура современного общества может быть парализована с появлением универсального квантового компьютера, поскольку *обычные алгоритмы шифрования использовать будет нельзя*. Уже сейчас Агентство национальной безопасности США (NSA) рекомендует переходить на *устойчивые к квантовому взлому криптографические алгоритмы*. Идут поиски путей создания постквантовой криптографии, устойчивой к квантовым вычислениям. И здесь также возникает масса не только технологических, но и правовых проблем.

Приложения

Генеральная Ассамблея Интерпола фокусируется на инновациях в полицейской деятельности

Дубай, Объединенные Арабские Эмираты. — «Полиция в век информации» является темой 87-й сессии Генеральной Ассамблеи Интерпола, всемирного мероприятия правоохранительных органов года, которое открылось в Дубае, Объединенные Арабские Эмираты (ОАЭ).

На этой четырехдневной конференции, собравшей около 1000 официальных представителей из 173 стран, включая 85 начальников полиции и почти 40 министров, будет рассмотрен вопрос о том, как технология изменит будущие угрозы и как она может использоваться правоохранительными органами для решения этих задач.

Поскольку более 55 процентов населения мира имеют доступ к Интернету, преступники все чаще используют данные в качестве средства для зарабатывания денег, о чем свидетельствуют недавние атаки вымогателей. Расширение использования искусственного интеллекта и робототехники, а также инноваций в области криминалистики тоже являются ключевыми вопросами для обсуждения.

Церемония открытия состоялась в присутствии вице-президента ОАЭ, премьер-министра и правителя Дубая — Его Высочества шейха Мухаммеда бен Рашида Аль Мактума.

Обращаясь к делегатам, Его Высочество шейх Саиф бен Заид Аль Нахайян, заместитель премьер-министра и министр внутренних дел, сказал: «Мы работаем вместе с нашими партнерами, чтобы обезопасить мир и сделать его более безопасным, содействуя усилиям по разработке проектов и инициатив Организации».

«Мы будем продолжать работать вместе, пока не одержим победу над терроризмом и преступностью». Старший вице-президент Интерпола Ким Чен Янг сказал, что решения, принятые офицерами Генеральной Ассамблеи стоят на переднем крае полицейской деятельности.

«В эпоху беспрецедентного обмена информацией полиция во всем мире все чаще сталкивается с новыми проблемами. «Собирая лучшие практики в рамках международной модели, Интерпол предоставляет нейтральную платформу с хорошими связями. Криминальные данные и правила их обработки стали критическими контурами для формирования работы международного полицейского сотрудничества »,— сказал г-н Ким. В целях содействия глобальному охвату Интерпола путем координации с региональными органами Генеральной Ассамблее будут представлены резолюции о сотрудничестве с Африполом и Совместной целевой группой «Группа 5» в Сахеле.

Генеральный секретарь Интерпола Юрген Сток сказал, что партнерские отношения с региональными органами сыграли важную роль в развитии сильной архитектуры глобальной безопасности. «С увеличением давления на правоохранительные органы мы должны избегать дублирования усилий, если мы хотим эффективно работать, чтобы сделать мир более безопасным»,— сказал генеральный

секретарь Шток. «Мы также должны использовать передовые технологии в интересах полиции по всему миру, и Интерпол обладает уникальными и идеальными возможностями для этого, особенно в плане предоставления жизненно важных биометрических данных во всем мире»,— добавил руководитель Интерпола.

Генеральный секретарь Сток сказал, что информация, полученная о самодельных взрывных устройств в Ираке и Персидском заливе, переданная через Интерпол, уже привела к идентификации подозреваемых в Европе и Азии.

В период с 18 по 21 ноября делегаты также получат обновленную информацию о трех программах преступной деятельности Интерпола: борьбе с терроризмом, киберпреступностью и организованной и возникающей преступностью, а также о связанных с ними оперативных успехах.

К ним относятся первая глобальная межведомственная операция по борьбе с загрязнением морской среды, изъятие 500 тонн запрещенных фармацевтических препаратов во время операции «Пангея XI» и операции «Эпервье», «Либертад» и «Савиян», в результате которых было спасено почти 1000 жертв торговли людьми и контрабанды людей. Заявки на членство от Кирибати, Косово и Вануату будут рассмотрены Генеральной Ассамблеей, которая также проголосует за нового Президента наряду с должностями в Исполнительном комитете для стран Америки, Азии и Европы в последний день конференции.

Генеральная ассамблея Интерпола одобряет план будущего организации

Кигали, Руанда. — Сегодня состоялось 84-е заседание Генеральной Ассамблеи Интерпола, в котором делегаты одобрили новую «дорожную карту» для будущего развития Организации, чтобы лучше поддержать свои 190 стран-членов в борьбе с трансляционной преступностью и терроризмом.

С рассмотрением INTERPOL 2020 об условиях Организации, стратегией, приоритетами и мероприятиями, получающими единодушную поддержку от делегатов, было решено, что Интерпол теперь будет работать со странами-членами для определения и разработки четкого набора результатов для укрепления своих полицейских возможностей, поддерживаемых сильными государственными механизмами.

Президент Интерпола Мирей Балестрази сказал делегатам, что их постоянная поддержка имеет важное значение для преобразования резолюций, принятых в ходе Генеральной Ассамблеи, в конкретные действия.

«Интерпол 2020 обеспечивает основополагающий элемент для развития Организации, и я призываю все страны-члены внести вклад в эту инициативу, которая поможет построить Интерпол будущего»,— сказала Президент Балестрази.

Генеральный секретарь Юрген Сток сказал, чтобы оставаться эффективным в решении текущих и возникающих угроз безопасности, важно укрепить все сферы деятельности Организации, как внутренние, так и внешние.

«Если Интерпол должен оставаться на авангарде глобальных усилий в области полицейской деятельности, важно, чтобы наши системы были надежными и отвечали на задачи, с которыми мы столкнемся в будущем», — сказал он.

«Интерпол предоставит нам стратегические рамки для обеспечения того, чтобы Организация оставалась сильным и уважаемым голосом в вопросах глобальной безопасности»,— добавил мистер Сток.

С развитием стратегических партнерских связей ключевым элементом инициативы Интерпол-2020, Генеральная Ассамблея поддерживает ряд резолюций для более тесного сотрудничества с частным сектором, в том числе посредством инициативы I–Checkit по усилению пограничного контроля.

Делегаты также одобрили рекомендацию Интерпол о том, чтобы поделиться своим проектом «Базового уровня» с частными сетями для поддержки промышленности и сетевых администраторов, чтобы распознавать, сообщать и удалять материалы о жестоком обращении с детьми из своих сетей.

Проект, который является частью базы данных Интерпола по международной сексуальной эксплуатации детей Интерпола, позволит отрасли перекрестно сопоставлять сигнатуры изображений, размещенные в их отчете, и удалять материалы о жестоком обращении с детьми из сетей в МСЭД.

Работа Интерпола по проекту «Основания» и дальнейшие разработки в базе данных ICSE будут представлены предстоящему глобальному саммиту #WeProtect Children Online, который состоится в Абу-Даби.

Объединения мировых лидеров, технологических компонентов и правоохранительных органов, двухдневное (16 и 17 ноября) мероприятие будет означать прогресс, достигнутый после инаугурационного события в Лондоне, в котором приняли участие около 50 стран и международных организаций, которые подписали заявление «We Protect» на высшем уровне.

База данных ICSE уже оказала помощь специалистам во всем мире, выявила более 7,700 жертв сексуального насилия среди детей и арестовала более 3,800 человек.

Была также обновлена общая ассамблея о ходе работы Рабочей группы по обработке информации (РГОИ), которая проводит всеобъемлющий обзор надзорных механизмов Интерпол на всех уровнях, включая национальные центральные бюро, Генеральный секретариат и Комиссию по контролю над Файлами Интерпола (ККФ).

В рамках продолжающегося процесса делегаты проголосовали за принятие ряда промежуточных мер для дальнейшего повышения, они являются уточненными стандартами в отношении использования странами-членами уведомлений и разъяснений в отношении стран-членов.

Генеральная Ассамблея, в которой приняли примерно 640 начальников полиции и старших должностных лиц правоохранительных органов из 145 стран, также избрали двух новых вице-президентов.

В 2016 году в Индонезии состоится 85-я сессия Генеральной Ассамблеи, и делегаты на этой неделе одобрили Китайский форум 86-й сессии 2017 года.

Интерпол привержен обеспечению того, чтобы правовые рамки Организации шли в ногу с технологическими разработками, и командой юристов в области информационно-коммуникационных технологий, которые специализируется на юридических проектах, связанных с законодательством ИКТ. Их деятельность сосредоточена вокруг шести ключевых областей:

1. Участие в проектах в области информационно-коммуникационных технологий с целью:

- включить Интерпол для оценки своей правовой базы в отношении будущих технологических разработок в области защиты данных, прав человека и конфиденциальности;
- быть передовыми в сфере правовых мер реагирования и событий, чтобы гарантировать, что новейшие технологические разработки имеют прочную правовую основу;
- предоставлять организации рекомендации по разработке правил и положений Интерпола, чтобы отразить технологические изменения в глобальном сообществе правоохранительных органов;
- предоставлять юридические консультации по внутренним проектам.

2. Поощряя сотрудничество между отделами Интерпола, включая Международный инновационный комплекс Интерпола, который осуществляется полицейскими проектами с использованием новых технологий.

3. Развитие Интерпола в качестве центра для юридических исследований, связанных с новыми технологиями.

4. Помощь в разработке типового законодательства, касающегося гарантий использования новых технологий.

5. Создание диалога и развитие партнерских отношений с научными кругами, частным сектором, представителями гражданского общества и правоохранительными органами.

6. Укрепление существующих отношений с другими международными организациями.

Технология беспилотных летательных аппаратов: угрозы безопасности и преимущества для полиции на форуме Интерпола

Беспилотный летательный аппарат «Сингапур» просвистел над головами толпы, сидящей в аудитории Глобального инновационного комплекса Интерпола (IGCI) в Сингапуре, выполняя воздушные маневры, демонстрирующие его способность работать в закрытых помещениях.

Второй показ продемонстрировал беспилотные летательные аппараты, предназначенные для использования в открытых пространствах, подчеркивая преимущества и проблемы развертывания такой технологии в общественных местах.

Технология беспилотников была на первом месте в IGCI на этой неделе во время трехдневной (28–30 августа) конференции экспертов по дронам, которая собрала около 100 экспертов из правоохранительных органов, научных кругов и частного сектора, чтобы продемонстрировать, как беспилотники могут одновременно стать и угрозой, особенно для критически важной инфраструктуры, и инструментом и источником доказательств для полиции всего мира.

Организованная Инновационным центром и контртеррористическим подразделением Интерпола при поддержке Федерального бюро расследований США (ФБР) и полиции Нидерландов, конференция стала первым шагом на пути к созданию глобального потенциала для борьбы с возникающей угрозой, исходящей от «беспилотных воздушных систем», известных как дроны.

С этой целью постоянное взаимодействие с экспертами в этой области поможет Интерполу облегчить обмен информацией, а также разработать набор руководящих принципов и оперативных процедур, которым должны следовать лица, оказывающие первую помощь, в случае инцидента с дроном, и помочь судебно-медицинским экспертам в извлечении данные от беспилотников для поддержки расследований. «Воздействие беспилотников на правоохранительную деятельность во всем мире продолжает расти. Ежедневно я слышу о новых агентствах, рассматривающих, как использовать их в правоохранительной деятельности; еженедельно я слышу об агентствах, принимающих их в связи с активными расследованиями; и кажется, что каждый месяц появляется новый поворот в угрозе беспилотников »,— сказал Стив Уотсон, генеральный директор VTO Labs, который выступил с основным докладом.

« Форум экспертов по дронам Интерпола собрал группу экспертов и практиков мирового уровня по теме беспилотных летательных аппаратов и их взаимосвязи с деятельностью правоохранительных органов. Интерпол продолжает находить способы проявить лидерство и вдохновение в новых технологических темах»,— заключил он.

Дроны как угроза

Потенциальное использование беспилотников в террористическом инциденте или нападении на критическую инфраструктуру и мягкие цели вызывает растущую обеспокоенность у правоохранительных органов, так как доступность технологии беспилотников становится все более распространенной в глобальном масштабе. Поскольку беспилотники становятся менее дорогими, и их потенциальное применение продолжает расширяться, ожидается, что страны будут свидетелями увеличения и развития этой угрозы.

Недавние примеры включают террористические группы, использующие беспилотники в целях наблюдения и доставляющие химические, биологические, радиологические, ядерные и взрывчатые материалы в зоны конфликта, и экологическую группу, которая перепрофилировала любительский беспилотник, чтобы войти в безопасное

воздушное пространство ядерной площадки и врезаться в выделенное здание, подчеркивают реальность угрозы, создаваемой незаконным использованием дронов.

В этом отношении эксперты из ФБР, НАТО, Контртеррористического исполнительного директората Совета Безопасности Организации Объединенных Наций, национальных полицейских учреждений и частного сектора подчеркнули необходимость скоординированного глобального реагирования правоохранительных органов, которое объединяет опыт и достижения различных стран, военные агентства и частную промышленность, чтобы противостоять угрозам, создаваемым бесчестным использованием дронов.

«Растущая угроза того, что террористические группы используют беспилотники для атаки на критически важные объекты инфраструктуры и« мягкие »цели, создала острую потребность в мировом правоприменительном сообществе для обмена информацией и передовым опытом. Интерпол стремится помогать своим странам-членам защищать их критически важную инфраструктуру путем повышения осведомленности, обмена передовым опытом и содействия обмену информацией о террористических инцидентах с участием беспилотников»,— сказал директор по борьбе с терроризмом Интерпола Патрик Стивенс.

Инструмент для полиции

Хотя беспилотники могут быть опасными в чужих руках, они также являются ценным инструментом для правоохранительных органов. Участники услышали, как полиция может использовать беспилотники для реконструкции места преступления, используя беспилотник, чтобы сфотографировать место со всех сторон, а затем подавать данные на 3D-принтер.

Беспилотники также могут использоваться правоохранительными органами для наблюдения, оказания помощи в расследовании дорожно-транспортных происшествий, обследования мест стихийных бедствий и многого другого.

Преобразование беспилотных летательных аппаратов и технологии искусственного интеллекта (ИИ) дает дополнительные преимущества для расширения текущих возможностей полиции: от повышения безопасности и производительности сотрудников полиции до трансляции инцидентов в режиме реального времени.

Источник доказательств

Беспилотники также могут быть важным источником доказательств в поддержку расследований и судебного преследования: анализ цифровых данных, таких как скорость, высота, координаты GPS и записи полета, могут выявлять информацию о вовлеченных преступниках, в то время как физические данные, такие как отпечатки пальцев и ДНК так же могут присутствовать.

Посредством дальнейшего развития этих возможностей Интерпол стремится оказывать странам-членам помощь в расширении обмена информацией об

инцидентах с беспилотниками и развитии их способности проводить эффективные судебные экспертизы захваченных беспилотников.

«Разные страны рассматривают технологию беспилотников по-разному: одни определяют дронов как оружие, а другие классифицируют их как самолеты. Кроме того, полиция начинает использовать беспилотники в качестве инструмента в своей повседневной работе»,— сказала Анита Хазенберг, директор Инновационного центра Интерпола.

«Эта конференция помогла объединить эти разные представления, выявить сходства и обменяться передовым опытом среди мирового сообщества о том, как одновременно рассматривать беспилотники как угрозу, инструмент и источник доказательств в полицейских расследованиях»,— заключила она.

Конференция основывается на результатах заседаний Рабочей группы по беспилотным операциям Интерпола в конце 2017 года и в начале 2018 года, которые заложили основу для сбора информации о проблемах и возможностях, которые беспилотники ставят перед правоохранительным органами

Инновации и технологии в полиции также будут занимать важное место в повестке дня сессии Генеральной Ассамблеи Интерпола в Дубае в ноябре.

На встрече экспертов Интерпола основное внимание уделяется вопросам сексуального насилия над детьми

Сингапур. — Эксперты по защите детей собрались в Сингапуре на этой неделе, чтобы определить меры по поощрению и поддержке правоохранительных органов во всем мире в выявлении жертв сексуального насилия над детьми.

Это было одним из вопросов, обсуждаемых Группой специалистов Интерпола по преступлениям против детей, которая собирается на ежегодной основе для обзора последних достижений в глобальных усилиях по борьбе с сексуальным надругательством над детьми в Интернете, выявлению молодых жертв и предотвращению распространения материалов о насилии.

Четырехдневное совещание (26–29 ноября) собрало 216 участников из 50 стран, региональных и международных организаций, частного сектора и научных кругов. Обсуждения во время встречи были сосредоточены вокруг четырех ключевых тем:

- Интернет-преступления против детей;
- Идентификация ребенка-жертвы;
- Управление сексуальными преступниками;
- Серьезные и насильственные преступления против детей.

С особым акцентом на поддержку полиции в развивающихся регионах в борьбе с сексуальным насилием над детьми в Интернете и защите жертв от дальнейшего вреда, участники обсудили новую целевую группу Интерпола по идентификации жертв в Азии, которая проведет свое первое совещание в следующем месяце в Сингапуре, и начали процесс оценки текущей ситуации в Африке с целью наметить курс для будущих действий.

Директор Интерпола по вопросам организованной и возникающей преступности Пол Стэнфилд сказал: «Хотя выявление жертв, изображенных на изображениях и видеофильмах о жестоком обращении с детьми, всегда будет в основе того, что делает Интерпол, мы также должны учитывать новые технологии, новые группы жертв и новые географические регионы риска. Наша цель — защитить самых уязвимых от самых опасных». В ходе встречи обсуждались также другие методы: методы предотвращения, использование мобильных устройств в преступлениях против детей, законодательство, касающееся сексуальных преступников и усовершенствования базы данных Интерпола по международной сексуальной эксплуатации детей (ICSE), которая в настоящее время содержит более 440000 изображений и видео. Тематические исследования выявили успехи, достигнутые странами в борьбе с преступлениями против детей.

Со времени своего создания в 1992 году Группа специалистов Интерпола по преступлениям против детей играла ключевую роль в глобальном развитии идентификации жертв в расследованиях с использованием изображений, связанных с жестоким обращением с детьми, благодаря своей активной роли в наращивании потенциала и повышении следственных стандартов реагирования правоохранительных органов на жестокое обращение с детьми во всем мире.

Интерпол проводит первую рабочую группу по DarkNet и криптовалютам

Альткоины определены как серьезная проблема для правоохранительных органов

Рост Альткойнов, альтернативы Биткойну, был определен как возникающая угроза первой Рабочей группой Интерпола по DarkNet и криптовалютам.

В последние годы Интерпол стал свидетелем резкого роста таких явлений, как рынки DarkNet, криптовалюты и специальные микшеры и тумблеры Биткойн, которые представляют серьезную угрозу, поскольку они не только связаны с киберпреступностью, но и охватывают множество криминальных областей.

Среди других проблем, выявленных участниками, были смесители криптовалют, методы анонимизации, отсутствие инструментов отслеживания альткойнов и децентрализованные услуги условного депонирования.

Рабочая группа, организованная в Глобальном комплексе инноваций Интерпола в Сингапуре в сотрудничестве с баварским министерством юстиции (Германия), собрала 39 участников, представляющих 18 стран-членов и Европол.

В ходе двухдневного совещания (15 и 16 марта) сотрудники полиции поделились примерами глобальных расследований по темным сетям и криптовалютам, а также техническими и юридическими проблемами, с которыми они сталкиваются в различных национальных контекстах.

Участники в подавляющем большинстве согласились с важностью создания сетей и обмена информацией для максимизации следственных ресурсов и предотвращения дублирования усилий. Рабочая группа обсудила использование разработанных криминалистических инструментов коммерческих и правоохранительных органов, и их преимущества при расследовании уголовных дел. Другие рекомендации включали использование баз данных и создание международных руководств по расследованию подобных преступлений.

Анита Хазенберг, директор Инновационного центра Интерпола, поддержала эту идею и призвала к активному сотрудничеству через Рабочую группу, которая будет служить глобальной платформой для борьбы с преступниками, которые стремятся использовать эволюцию методов анонимизации.

Собрание также подтвердило, что наращивание потенциала и обучение в DarkNet и криптовалютах имеют решающее значение для обеспечения того, чтобы следователи следили за развитием инструментов и методов судебной экспертизы. Вторая рабочая группа состоится в октябре 2018 года в Германии.

Глобальное полицейское сообщество одобряет меры по укреплению глобальной безопасности

Лион, Франция. — Роль технологических изменений, направленных против терроризма и транснациональной преступности, была подчеркнута в ключевых мерах, одобренных руководителями полиции всего мира на 14-м ежегодном совещании глав Национальных Центральных Бюро (НЦБ) Интерпола.

Делая акцент на инновациях в сфере охраны правопорядка и безопасности, делегаты трехдневной конференции (10–12 апреля) стремились укрепить международное сотрудничество среди полиции путем разработки инструментов и программ полицейской деятельности, специально предназначенных для региональных потребностей.

Модернизация стимулирующая исследования.

Учитывая, что распознавание лиц является важным и быстро развивающимся биометрическим инструментом для выявления подозреваемых в совершении преступлений и оказания помощи в раскрытии преступлений, старшие должностные лица полиции подчеркнули необходимость добавления изображений лиц в базу данных Интерпола по распознаванию лиц и предоставления подразделениям пограничного контроля большего доступа к глобальным биометрическим услугам Интерпола. В этом отношении обзор проекта Интерпола FIRST («Лицевое, Визуализированное, Распознавание, Поиск и Отслеживание») дал ценную информацию о том, как обмен биометрическими данными о подозреваемых в терроризме может помочь повысить национальную и региональную безопасность посредством обмена биометрическими данными. На совещании было озвучено, как в ходе полевой операции Project FIRST в Нигере изображения лиц, отпечатки пальцев

и ДНК, взятые у 179 заключенных, привели к двум совпадениями в базах данных Интерпола. В результате одного из них заключенный, арестованный в тренировочном лагере террористов, идентифицировался как тот же человек, который был отпечатан в малийской тюрьме в 2014 году. Аналогичным образом, полиция в Буэнос-Айресе недавно арестовала находившегося в международном розыске подозреваемого в убийстве после того, как его изображение было идентифицировано как вероятное совпадение подразделением Интерпола по распознаванию лиц.

Проект будущей глобальной полицейской деятельности.

В рамках программы реформ Интерпола 2020 Генерального Секретаря, НЦБ также были проинформированы о текущих усилиях по расширению основных услуг Интерпола посредством всестороннего обзора возможностей для повышения эффективности современных правоохранительных органов в мире, включая:

- Twinning: программа Интерпола, позволяющая странам использовать активы, передовой опыт и ресурсы друг друга, чтобы полиция во всех регионах работала на полную мощность.
- Проект стандартов качества НЦБ: онлайн инициатива, позволяющая странам самостоятельно оценивать свое соответствие рабочим стандартам Интерпола и позволяющая Генеральному Секретариату оказывать специализированную поддержку в случае необходимости.
- Служба онлайн-перевода полиции: важнейший инструмент для многоязычной организации, требующей быстрых круглосуточных действий полиции в безопасной среде, адаптированной специально к международной терминологии полиции.
- I–Core: инициатива по обзору для обеспечения того, чтобы новые глобальные полицейские службы Интерпола производились, интегрировались, управлялись и предоставлялись согласованно и в соответствии с потребностями глобального правоохранительного сообщества.

Мемориал Интерпола

В течение трех дней встречи участники почтили память погибших полицейских по всему миру у мемориала, который Интерпол недавно открыл в штаб-квартире Генерального Секретариата в Лионе, а также в Глобальном комплексе инноваций Интерпола в Сингапуре.

Ransomware — новый вызов цифровой безопасности Интерпола

Сингапур. — В последнем издании Interpol Digital Security Challenge участники выслеживали подозреваемого, который зашифровал конфиденциальные медицинские записи с помощью ransomware (вредоносное программное обеспечение, которое работает как вымогатель. После установки на компьютер жертвы,

программа зашифровывает большую часть рабочих файлов (например, все файлы с распространенными расширениями).

Следователи по киберпреступности и эксперты в области цифровой криминалистики из 20 стран и территорий были разделены на команды, участвующие в гонках на время и друг против друга, чтобы раскрыть преступление, установить подозреваемого и собрать достаточно доказательств для успешного судебного преследования.

Целью данного упражнения является создание реалистичной моделируемой среды для специалистов для дальнейшего развития их знаний и обмена опытом в расследовании киберпреступлений.

Ransomware — один из наиболее быстро растущих типов вредоносных программ. В отчете Trend Micro показано, что в 2016 году число новых программ составило 752% по сравнению с предыдущим годом.

Используя ПК и ноутбуки, предварительно загруженные целым рядом цифровых инструментов криминалистической экспертизы, команды получали очки за каждый успешный этап расследования, которое началось с «больницы», обратившейся за помощью в полицию.

Соревнования

В этом сценарии следователи сначала определили, какой компьютерный терминал в больнице был заражен, и установили, что это произошло с помощью «дроппера» (типа вредоносного ПО для запуска вирусов) из электронного письма, содержащего подозрительную ссылку.

После идентификации сервера управления и контроля, который был связан с вымогателем, команды проанализировали журнал доступа, который привел их к IP-адресу, связанному с домашним провайдером подозреваемого, и его телефон был изъят. Анализ данных телефона показал, что он использовался для отправки электронного письма, содержащего «дроппеа», для заражения компьютера в больнице. Дальнейший анализ показал предыдущее подключение к бесплатному Wi-Fi-сервису в близлежащем аэропорту, который также использовался для подключения к вымогателям.

Несмотря на то, что это не являлось частью самой задачи, участникам была представлена презентация корпорации NEC о программном обеспечении для распознавания лиц и его потенциальном использовании в кибер-расследованиях для соединения виртуальных и физических доказательств, как это могло бы быть в аэропорту.

Расследование киберпреступлений становится все более сложными, и эта проблема повторяла некоторые повороты, с которыми сталкиваются следователи каждый день»,— сказал Нобору Накатани, исполнительный директор Глобального инновационного комплекса Интерпола (IGCI), который принимал участие в этой соревновании.

«Наряду с предоставлением участникам навыков, необходимых для проведения эффективных расследований, задача цифровой безопасности также подчеркивает необходимость тесного сотрудничества с частным сектором, которое было идеалом IGCI с тех пор, как мы впервые открыли свои двери»,— добавил г-н Накатани.

Развитие опыта при поддержке частного сектора

Соревнования были организованы в тесном сотрудничестве с корпорацией NEC и Институтом киберзащиты, что способствовало разработке сценария. Четырехдневное мероприятие (14–17 марта) включало в себя учебные занятия по выработке практических знаний участников по различным вопросам, от выявления вредоносных программ до аналитики биткойнов, которые проводили специалисты из частного сектора из Cellebrite, LAC, Meiya Pico, SECOM и TrendMicro

Digital Security Challenge стал очень практической демонстрацией приверженности Интерпола делу совершенствования навыков следователей в области кибербезопасности во всем мире. NEC рада, что снова помогла в разработке этого перспективного мероприятия и предоставила Интерполу наш опыт»,— сказал Казухико Шираиши, генеральный директор подразделения решений задач национальной безопасности корпорации NEC.

Президент Института киберзащиты Кенджи Хиронака сказал: «Институт киберзащиты гордится тем, что предоставлял криминалистическую информацию и техническую поддержку на протяжении всего этого мероприятия, которое было столь же успешным, как и первое».

По прогнозам, к 2020 году 21 млрд. устройств, используемых предприятиями и потребителями во всем мире, будут подключены к Интернету, задача является одной из нескольких инициатив, предпринятых IGCI, чтобы помочь странам-членам развить готовность и опыт в области кибербезопасности.

В дополнение к основным соревнованиям по цифровой безопасности, организуемым в IGCI, Интерпол также тесно сотрудничает со странами-участницами в проведении национальных мероприятий «@Your Site», первые из которых были проведены в Токио, Япония, в феврале этого года.

Европейский комитет по преступлениям. Концепция

Название проекта: искусственный интеллект и уголовно-правовая ответственность в государствах-членах Совета Европы — пример автоматизированных транспортных средств

ОБЛАСТЬ ПРОЕКТА: Государства-члены Совета Европы

БЮДЖЕТ: Примерно семьсот шестьдесят пять тысяч евро (765000 €)

ПРОДОЛЖИТЕЛЬНОСТЬ: 2 года

РЕАЛИЗАЦИЯ: Управление информационного общества и борьбы с преступностью — DGI, Совет Европы

Проект Совета Европы по искусственному интеллекту (ИИ)[1] и уголовно-правовой ответственности

Анализ проблем и оценка потребностей

После некоторых инцидентов с автоматизированными транспортными средствами в государствах-членах Совета Европы[2] и за его пределами[3] был задан следующий вопрос: кто будет нести ответственность, если полностью автоматизированное транспортное средство[4] ранит или убивает человека? При использовании алгоритмов самообучения за рулем автомобиля возникает более общий вопрос: как уголовное законодательство должно учитывать искусственный интеллект (ИИ)?

Долгосрочные тенденции в технологическом развитии, а также в случае с автоматизированными транспортными средствами, позволяют предположить, что ИИ и машины с автономной функциональностью будут все более широко представлены в развитых обществах, и что государствам следует задуматься над тем, как справиться с этим, в рамках своих правовых и нормативных актах. Первый существенный шаг уже сделан с введением технических стандартов для специальных разрешений, разрешающих автоматическое вождение в национальных юрисдикциях, но некоторые юрисдикции придерживаются позиции, что для деятельности, которая не считается незаконной[5], разрешение не требуется. При пересечении границ, как представляется, в интересах государств-членов Совета Европы предусмотреть, как его стандарты могут быть адаптированы таким образом, чтобы обеспечить их сотрудничество в будущих случаях, если автоматизированные транспортные средства станут причиной аварий в других странах или незаконной деятельности, влияет на более чем одну юрисдикцию.

К сожалению, крайне маловероятно, что риск несчастных случаев упадет до нуля[6]. Также можно предвидеть, что некоторые люди будут злонамеренно

[1] Не существует согласованного определения искусственного интеллекта (ИИ), но для целей настоящего документа Совет Европы признает этот термин как охватывающий системы, которые работают и способны выполнять сложные задачи, цель которых состоит в том, чтобы добиться имитации машиной познавательных способностей человека. https://www.coe.int/en/web/human-rights-rule-of-law/artificial-intelligence

[2] Например, несчастные случаи, связанные с вспомогательным вождением в Германии (AG München, Urteil vom 19. 7. 2007–275 C15658/07), Норвегия <https://newatlas.com/tesla-autopilot-fema/46045> или Швейцария (https://www.nzz.ch/panorama/tesla-fahrer-will-nach-unfall-milderes-urteil-ld.1334364), а также https://www.youtube.com/watch?v=qQkx-4pFjus или автономное вождение в Швейцарии https://www.swissinfo.ch/rus/autilitary-post-bus-gets-in-accident/42467476

[3] Голландский организация по утверждению транспортных средств RDW, по-видимому, обратилась в Национальное управление безопасности дорожного движения США (NHTSA) за подробностями после фатальной аварии Tesla, чтобы выяснить, безопасны ли автомобили, оснащенные функцией автопилота, одобренные в Европе RDW. Http: / /fortune.com/2016/07/14/tesla-crash-netherlans

[4] В соответствии со стандартом SAE J3016_201806 <https://www.sae.org/standards/content/j3016_201806/> различают шесть уровней автономии, начиная с уровня 0: нет автоматизации; уровень 1: помощь водителю; уровень 2: частично автоматическое вождение; уровень 3: высокоавтоматическое вождение; уровень 4: полностью автоматизированное вождение; уровень 5: полная автоматизация (без водителя).

[5] См. например: информационный список разрешений, предоставленный Федеральным дорожным управлением Швейцарии FEDRO / ASTRA <https://www.astra.admin.ch/astra/de/home/themen/intelligente-mobilitaet/pilotversuche.html>.

[6] Несчастные случаи все еще происходят: Дайсуке Вакабаяши «Самодвижущийся автомобиль Uber убивает пешехода в Аризоне, где бродят роботы» The New York Times (19 марта 2018 года), доступно на https://www.nytimes.com/2018/03/19 / технологии / убер-машинистов-fatality.html; Брайант Уолкер Смит «Автоматическое вождение и ответственность за качество продукции», Мичиганское юридическое обозрение (2017), доступно по адресу: https://digitalcommons.law.msu.edu/cgi/viewcontent.cgi?article=1187&context=lr

использовать искусственно интеллектуальные устройства для совершения уголовных преступлений[7].

Во время написания статьи ИИ и автоматизированные транспортные средства в основном использовались в ограниченных, контролируемых обстоятельствах. Среди прочего, это связано с тем, что машинное обучение может быть реализовано по-разному, и европейские страны выбрали «медленный подход»[8]. Однако растущее присутствие ИИ в гражданской жизни ставит ряд сложных вопросов для правовых систем Европы. Несмотря на то, что этим тенденциям присуща непредсказуемость, текущие прогнозы показывают, что в течение следующих пяти — десяти лет автоматизированные транспортные средства, станут гораздо более распространенными в повседневной жизни, на транспорте и в промышленности[9], и, хотя и обещают существенные преимущества в плане безопасности, не смогут предотвращать все несчастные случаи. Преимущество установления четких общих правил уголовной ответственности будет способствовать надлежащему отправлению правосудия.

Относительно простой вопрос о том, кто должен быть привлечен к уголовной ответственности за вредные последствия в результате автономных процессов принятия решений машиной, не всегда имеет простой ответ. В уголовном праве трудно иметь дело с «преступным поведением» нечеловеческих существ; если ИИ займет место водителя, может возникнуть разрыв в ответственности. Одна из основополагающих целей этого проекта и его потенциальных результатов заключается в оценке необходимости введения согласованных положений между государствами для определения ситуаций уголовной ответственности, в частности в ситуациях аварий, вызывающих серьезный ущерб, и, таким образом, для предотвращения нежелательных последствий для безопасного использования этих передовых технологий и предотвращение возможных неблагоприятных воздействий.

Хотя в академических исследованиях и умозрительной фантастике уже давно ведутся этические дебаты относительно потенциальных преимуществ и опасностей искусственно интеллектуальных машин, проведен сравнительно небольшой институциональный анализ того, как реально решить конкретные проблемы уголовной ответственности, которые могут возникнуть в ближайшие годы. Вопрос об уголовной ответственности иллюстрирует то, что правовая основа, применяемая в настоящее время для разработки и использования автоматизированных транспортных средств (или другого ИИ), основана на нормативных

[7] https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes; https://www.bleepingcomputer.com/news/security/volkswagen-and-audi-cars-vulnerable-to-remote-hacking

[8] https://www.bloomberg.com/news/articles/2018–03–20/it-s-a-good-thing-europe-s-autonomous-car-testing-is-slow

[9] Например, IHS Markit прогнозирует, что миллионы автомобилей «с той или иной формой автономии» будут производиться и продаваться в течение ближайшего десятилетия, при этом рынок может достичь 600000 автомобилей в 2025 году и потенциально до 21 миллиона автомобилей, продаваемых в год в 2035 году. Точно так же ожидается быстрый рост промышленной робототехники, так как общий объем продаж интеллектуальных автономных машин увеличивается в среднем на 12% в год по всему миру.

принципах, разработанных в до — цифровую эпоху. В результате в различных ситуациях неясно, как и когда можно определить ответственность за нанесенный вред. В интересах обеспечения адекватных средств подотчетности в ситуациях, когда автоматизированные транспортные средства (или другой ИИ) могут нанести вред человеку, необходимо помочь создать четкую уголовно-правовую базу.

Поэтому было бы полезно заранее установить правила, регулирующие любую потенциальную уголовную ответственность, чтобы гарантировать, что в таких случаях, как автомобильное столкновение или авария с дроном, ни одному государству не придется сталкиваться с неясной правовой ситуацией из-за неподходящей или устаревшей правил. Этот проект также имеет целью, учитывая характер предельного соотношения уголовного регулирования в этой сложной области, рассмотреть обстоятельства, при которых степень вреда или важность нарушенного обязательства могут или должны привести к уголовной ответственности.

Поскольку потенциальное широкое внедрение автоматизированных транспортных средств затронет все государства-члены Совета Европы и за его пределами, Организация должна сыграть определяющую роль в содействии разработке общих принципов, касающихся ИИ. Что касается более конкретного вопроса об уголовно-правовой ответственности, то Европейский комитет по уголовным проблемам (CDPC) Совета Европы может помочь государствам разработать общие правовые стандарты, обеспечивающие адекватную, всеобъемлющую и понятную систему регулирования, которая при одновременном признании многими полезного использования автоматических транспортных средств, также гарантирует четкую основу для устранения возможных злоупотреблений и вредных последствий ИИ. Чтобы поддерживать хорошее сотрудничество по уголовным делам между членами Совета Европы, необходимо решить несколько вопросов, включая вопрос о том, как различные подходы в тестировании и использовании автоматических транспортных средств могут привести к «допустимым рискам», не криминализированным в национальном законодательстве (как различные виды использования технологий в автомобилях), а также вопрос о том, может ли автоматизированное транспортное средство в конечном итоге отвечать закону как электронное лицо (подобно корпорациям как юридическим лицам), или же уголовное правосудие предназначено только для «людей».

В этом процессе должен участвовать ряд участников, включая, например, регулирующие органы, такие как министерства транспорта или органы безопасности дорожного движения, и другие, которые разрабатывают и внедряют стандарты и процедуры безопасности для определения соответствия нормативным требованиям для автоматизированных транспортных средств.

Технологические стандарты, разработанные на международном уровне[10], могли бы затем проложить путь к надлежащему тщательному правовому регулированию

[10] См. например: Таксономия и определения терминов, связанных с системами автоматизации вождения для дорожных транспортных средств J3016_201609 <https://www.sae.org/standards/content/j3016_201609/>, упоминаемых в Общем подходе ЕС к правилам ответственности и страхованию для связанных и автономных транспортных средств

на национальном уровне, касающемуся использования и контроля над автоматизированным вождением, включая принципы распределения уголовно-правовой ответственности за использование ИИ и соответствующие санкции и меры, где это необходимо, а также общая правовая база для решения любых трансграничных проблем и правовая основа для содействия взаимной правовой помощи по уголовным делам.

2. Обоснование

2.1 Ответственность ИИ и уголовного права: пример автоматизированного (самостоятельного вождения) транспортного средства и уголовная ответственность

К сожалению, тысячи жертв дорожно-транспортных происшествий происходят каждый день по всему миру. Согласно многочисленным исследованиям человеческая ошибка является наиболее частой причиной несчастных случаев. Однако в типичных дорожно-транспортных происшествиях определение, какая сторона или стороны виноваты, часто является сложной задачей.

19 марта 2018 года автоматизированный внедорожник убил женщину на улице в Аризоне. Она стала первым пешеходом, который, как известно, был убит автоматическим транспортным средством[11]. Во время аварии машина с автоматическим управлением находилась в автоматическом режиме и ударила женщину, которая шла по улице за пределами тротуара. Во время аварии внутри машины находился оператор автомобиля.

Как обычно в этих случаях, полиция должна провести расследование, чтобы понять причину аварии. Первые вопросы: водитель ехал слишком быстро? был ли он / она под влиянием алкоголя? или наркотиков? Но в деле в Аризоне был только водитель безопасности. Здесь мы впервые сталкиваемся с ситуацией, когда автоматический автомобиль убил человека.

Все эти инциденты поднимают один и тот же вопрос; вопрос, который задавался много раз раньше: кто является ответственной стороной или сторонами? Производители автомобилей? Лицо / орган, который предоставил разрешение на проведение испытаний? Водитель в салоне автомобиля во время аварии? Что очень ясно, так это то, что для многих людей нет однозначного ответа на этот вопрос; напротив, другие считают, что даже ответственную сторону или стороны определить проще, поскольку доступно больше данных.

<www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU (2018) 615635>, с. 42; Международная организация по стандартизации (ИСО) <https://www.iso.org/fr/home.html>; ИТЦ ЕЭК ООН WP1, который является глобальным форумом по безопасности дорожного движения <https://www.unece.org/trans/areas-of-work/road-traffic-safety/meetings-and-events/global-forum-for-road -безопасность-трафика-wp1.html>; ИТЦ ЕЭК ООН WP29, который является Всемирным форумом ЕЭК ООН по согласованию правил в области транспортных средств https://www.unece.org/trans/main/wp29/introduction.html

[11] Брайант Смит Уокер, «Смертельная катастрофа Убер», Стэнфордская юридическая школа (19 марта 2018 года), доступно по адресу: <https://cyberlaw.stanford.edu/blog/2018/03/ubers-fatal-crash>.

Автоматизированные транспортные средства явно эксплуатируются компаниями, разрабатывающими технологии, но как только транспортные средства приобретаются и принадлежат частным лицам, картина виновных становится еще более неясной. Некоторые вопросы ответственности будут решены до того, как власти будут утверждать автоматические транспортные средства для общественного движения. Но простой вопрос о том, кого привлекать к уголовной ответственности за вредоносные последствия автономных процессов принятия решений машиной, не всегда дает простой ответ.

2.2 Ключевые вопросы уголовного права и искусственного интеллекта

Как уже упоминалось, для большинства технологических разработок можно смело предположить, что ранее существовавшие принципы и нормы уголовного права будут достаточными для обеспечения ответственности за серьезный вред и другие формы недопустимого поведения. Тем не менее, это может быть не совсем верно в отношении искусственного интеллекта, поскольку сложность и сложность автономного принятия решений и самообучения в основе технологии могут оставить пробел в ответственности.

Во всех государствах-членах Совета Европы уголовное право, как правило, рассматривается как относящееся к поведению и намерениям людей, действующих в качестве физических лиц или действующих от имени юридических лиц (корпоративная ответственность). Этот проект связан с материальным уголовным правом, применимым на всех этапах разработки и использования автоматизированных транспортных средств.

Сложность, присущая этим высокотехнологичным системам может привести к значительным недоразумениям и заблуждениям для многих проектировщиков, производителей, регуляторов и пользователей, что делает необходимым, чтобы все соответствующие стороны знали о своих соответствующих правах и обязанностях.

Неоднозначность и отсутствие точности в этих продвинутых процессах принятия решений могут представлять серьезные проблемы как фактического, так и правового характера при определении источника ошибки, которая привела к причинению вреда или ущерба. Хотя современное поколение интеллектуальных автономных роботов способно принимать ограниченную степень автономных решений, приводящих к внешним воздействиям, уже трудно окончательно определить причину нанесения каждого ущерба. Тем не менее, следующее поколение самообучающихся роботов и транспортных средств с самообслуживанием создает значительные проблемы, которые могут усложнить установление причинно-следственной связи.

2.3 Сотрудничество и координация

Определение соответствующих стандартов для безопасного и полезного использования искусственного интеллекта является глобальной проблемой, и ей можно эффективно противостоять только путем расширения сотрудничества

и координации не только между государствами-членами, но и между различными международными организациями и соответствующими форумами.

Координация деятельности с этими и другими соответствующими партнерами, включая частный сектор, опираясь на работу друг друга и избегая ненужного дублирования, является явным приоритетом, с тем чтобы Совет Европы мог повысить ценность текущих усилий в этих чрезвычайно сложных вопросах.

3. Заинтересованные стороны

Государства-члены несут основную ответственность за обеспечение соответствия многих видов применения искусственного интеллекта международным и национальным правовым стандартам. Предполагается, что любой процесс установления нормативных стандартов в этой области также потребует участия ряда заинтересованных сторон, включая, но не ограничиваясь:

Система уголовного правосудия:

- Прокуроры и следователи,
- Суды первой инстанции,
- Министерство юстиции / центральные администрации.

Образование и академия:

- инженеры робототехники,
- этики,
- юристы (технологическое право, информационное право, юристы по уголовным делам).

Гражданские власти:

- Регулирующие органы,
- Государственные автономные системы (гражданские, а не военные),
- Государственные инфраструктурные системы.

Частные лица:

- Производители робототехники,
- Программисты и разработчики программного обеспечения,
- Частные компании,
- Исследователи ИИ и фирмы-разработчики.

4. Цели и задачи

Целью этого проекта является определение принципов и правил, касающихся уголовной ответственности физических и юридических лиц за вред и ущерб, причиненный автономными технологиями в гражданском контексте[12], и в частности, автоматизированными транспортными средствами.

Таким образом, цели проекта заключаются в следующем:

[12] Ссылка на гражданский контекст предназначена прежде всего для обозначения невоенного контекста: этот проект не касается использование автономных функций вооруженными силами государств-членов.

1. Изучить и выяснить нынешний существующий охват и содержание соответствующих национальных уголовных законодательств и международного права, касающиеся использования автоматических транспортных средств (или других ИИ), а также для определения, где и как созданы регулирующие полномочия в компетентных национальных государственных органах.

2. Определить, где конкретное поведение имело место и должно быть запрещено и криминализировано в отношении к делегированию, разделению или назначению задач, функций и поведения автономных технологий и при каких обстоятельствах.

3. Установить, где применимы принципы и нормы для физических или юридических лиц за вред, причиненный автоматизированными транспортными средствами (или другим ИИ).

4. Изучить сферу действия и содержание международно-правового документа для обеспечения общего стандарта уголовно-правовых аспектов автономных технологий и вреда, причиненного искусственного интеллектуальные в процессе принятия решений, в частности, автоматизированными транспортными средствами.

Каждая из этих четырех основных целей проекта, действий и ожидаемых результатов будет более подробно рассматривается ниже.

5. Индикативное логическое вмешательство

IMPACT — гармонизированные принципы и правила относительно уголовной ответственности за автоматизированные транспортные средства (или другие ИИ) по всей территории Совета Европы.

5.1 Общие итоги и результаты проекта

Общим итогом этого проекта будет создание международного документа по правонарушениям, связанным с вредом, причиненным в контексте использования искусственного интеллекта и, в частности, автоматизированными транспортными средствами, которые будут построены на основе оценки существующих международных правовых рамок и национальных уголовных законов стран-членов Совета Европы. Проект структурирован по четырем основным результатам:

Результат 1

5.1.1 Исследовательский проект по национальному уголовному праву и международно-правовой базе, применимым к автоматизированным транспортным средствам (или другим ИИ)

Деятельность: Анкета с последующей подборкой ответов и анализом.

Причины: Для изучения существующей нормативной базы в области искусственного интеллекта, автоматических машин и, в частности, автоматических транспортных средств, ключевая информация на национальном уровне должна быть получена от государств-членов.

Ожидаемый результат: Итоговый документ будет содержать исчерпывающую перепись соответствующих национальных и международных правовых подходов и инструментов для проведения всестороннего анализа.

Результат 2

5.1.2 Международная конференция по нормам общего уголовного права в отношении вреда, причиненного автоматизированными транспортными средствами (или другим использованием ИИ)

Деятельность: На основе приведенного выше анализа соответствующих национальных и международных правовых подходов и инструментов должна быть организована международная конференция, обеспечивающая форум, на котором государства-члены, а также субъекты государственного и частного секторов обсуждают события в области автоматизированных транспортных средств (или другого ИИ), пробелы в существующем уголовном праве, уже существуют решения в области уголовного права и есть ли возможность для формирования международного документа по уголовно-правовым аспектам искусственного интеллекта. Вклад эксперта является важным аспектом проекта для обеспечения того, чтобы на ранней стадии направление проекта и его основное содержание основывались на самых последних и наилучших исследованиях и знаниях по данному вопросу.

Методы работы: Международная конференция, объединяющая государства-члены и государства, не являющиеся членами, субъекты частного сектора и научные круги.

Ожидаемый результат: Выводы о необходимости разработки международного документа, устанавливающего общие правовые стандарты в этой области.

Результат 3

5.1.3 Экспертная редакционная группа для разработки документа, устанавливающего общие нормы уголовного права в отношении вреда, причиненного автоматизированными транспортными средствами (или другим ИИ)

Деятельность: На основе анализа соответствующего национального и международного законодательства и выводов международной конференции Совет Европы мог бы создать специальную редакционную группу национальных экспертов для разработки международно-правового документа, предусматривающего надлежащее уголовно-правовое регулирование использования автоматизированных транспортных средств (или другого ИИ).

Причины: Такой международный документ мог бы помочь обеспечить общую правовую основу для регулирующей деятельности государств-членов, обеспечить стандарты международного сотрудничества и общего уголовного права между

государствами-членами, а также способствовать взаимной правовой помощи и международному сотрудничеству по уголовным делам.

Методы работы: Рабочая / редакционная группа, состоящая из представителей государств-членов, будет встречаться несколько раз в течение определенного периода.

Ожидаемый результат: Будет подготовлен международный документ об уголовных преступлениях, связанных с вредом, причиняемым искусственным интеллектом и, в частности, автоматизированными транспортными средствами.

Результат 4

5.1.4 Международная конференция по случаю принятия нового международного документа о вреде, причиненном автоматизированными транспортными средствами (или другим ИИ)

Деятельность: Международная конференция по запуску нового документа, повышению осведомленности о существовании документа и предоставлению объяснений и информации о его положениях и целях.

Методы работы: Конференция с участием многих заинтересованных сторон, в которой принимают участие государства-члены и государства, не являющиеся членами, субъекты частного сектора и научные круги.

Ожидаемый результат: Повышение осведомленности о новом международном документе. Государства обновляют действующее законодательство и / или разрабатывают новое законодательство в соответствии с положениями нового документа.

Парламентская Ассамблея Совета Европы

Документ 14628
26 сентября 2018

Правосудие по алгоритму — роль искусственного интеллекта в системах охраны правопорядка и уголовного правосудия

Предложение о рекомендации.

Выступили Борис Чилевич и другие члены Ассамблеи.

Это предложение не обсуждалось на Ассамблее и распространяется только на тех, кто его подписал.

Система уголовного правосудия представляет собой одно из центральных направлений государственной деятельности, обеспечивающее общественный порядок, предотвращение нарушений различных основных прав, а также выявление, расследование, судебное преследование и наказание за совершение уголовных преступлений. Оно предоставляет властям значительные принудительные полномочия, включая слежку, арест, обыск и арест, задержание и применение физической и даже силы, влекущей за собой летальный исход.

Инструменты обработки данных все чаще используются в системах уголовного правосудия. Самые передовые системы используют прогнозирующие алгоритмы для информирования процесса принятия решений в таких областях, как типы полицейской деятельности, залог и приговор. Они во многом доказали свою эффективность и часто ценятся властями, которые их используют.

Однако есть основания для беспокойства. Эти системы обычно предоставляются частными компаниями, и в этом случае алгоритмы являются коммерческими секретами — «черными ящиками», которые не могут быть предметом общественного контроля. Качество вывода алгоритма зависит от качества входных данных: если входные данные непреднамеренно отражают, например, расовую предвзятость, то же будут делать и выходные данные, несмотря на кажущуюся нейтральность и объективность алгоритма. Лица, принимающие решения, могут неохотно отходить от рекомендаций, генерируемых алгоритмами, в ущерб зачастую важной роли индивидуального суждения и усмотрения. Полицейские департаменты могут потерять контроль над своими собственными данными, что делает их зависимыми от частных компаний, которые их приобрели, без особого выбора, кроме как поддерживать договорные отношения любой ценой.

Парламентская ассамблея должна изучить роль алгоритмов и искусственного интеллекта в системах уголовного правосудия с точки зрения стандартов Совета Европы о правах человека и верховенстве права с целью выработки возможных рекомендаций государствам-членам и Комитету министров относительно дальнейших действий.

Юрий Жданов,
Владимир Овчинский

Полиция будущего

Подписано в печать 26.12.2018. Формат 60x90 1/16.
Печать цифровая. Бумага офсетная.
Тираж 7000 экз.