ЕЛЕНА ЛАРИНА
ВЛАДИМИР ОВЧИНСКИЙ

ЦИФРОВАЯ РЕВОЛЮЦИЯ

ПРЕИМУЩЕСТВА И РИСКИ

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ
И ИНТЕРНЕТ ВСЕГО

Елена Сергеевна Ларина
Владимир Семенович Овчинский

Цифровая революция. Преимущества и риски. Искусственный интеллект и интернет всего

Текст предоставлен издательством
http://www.litres.ru/pages/biblio_book/?art=68832966
Цифровая революция. Преимущества и риски. Искусственный интеллект и интернет всего: Книжный мир; Москва; 2022
ISBN 978-5-6048263-6-2

Аннотация

За прошедшие годы технологии произвели революцию в нашем мире и в повседневной жизни. Компьютеры стали быстрее, портативнее и мощнее, чем когда-либо прежде. Произошел революционный взрыв небывалых технологий. Это касается искусственного интеллекта, Интернета вещей, Интернета тела, Интернета всего, – а также криптовалюты и блокчейна, квантовых вычислений и 5G – нового стандарта мобильной связи пятого поколения.

Технологии становятся все более сложными и все более взаимосвязанными. Автомобили, самолеты, медицинское оборудование, финансовые транзакции и системы электроснабжения – все они зависят от большого количества компьютерных программ, что делает их одновременно более сложными для восприятия и, в большинстве случаев, более трудными для контроля. Эта растущая сложность делает все более важным понимание, что технологические достижения меняют жизнь во всем мире как в положительную, так и в отрицательную сторону.

Авторы книги, которая предлагается вашему вниманию, исходят из тезиса, что любая сверхсовременная технология может использоваться в тройном назначении: во-первых, государством и обществом – для социального и экономического развития; во-вторых, – военными структурами, правоохранительными органами и спецслужбами – для повышения эффективности боевого потенциала армии, обеспечения общественной и государственной безопасности. И это во благо. Но есть и третья сторона. Достижения современной науки используются также криминальными и террористическими структурами – для совершения преступлений, нанесения ущерба государству, обществу, личности.

Есть ли способ защититься от кибератак злоумышленников? Какая страна сегодня может называться кибердержавой? И каково место России в этой гонке? Основываясь на богатом фактическом и исследовательском материале, авторы дают исчерпывающие ответы на самые острые вопросы.

В формате PDF A4 сохранен издательский макет книги.

Содержание

Владимир Овчинский, Елена Ларина Цифровая революция. Преимущества и риски. Искусственный интеллект и интернет всего

© Ларина Е.С. 2022
© Овчинский В.С, 2022
© Книжный мир, 2022
© ИП Лобанова О.В., 2022

Введение

Время в истории человечества, в которое мы живём, не похоже ни на какое другое. По мере того, как мир переживает период цифровой трансформации, мы быстро раскрываем потенциал технологий для улучшения жизни и решения некоторых из величайших проблем человечества. Это стало особенно очевидным в 2020-2021 годах, когда страны повсюду боролись с последствиями глобальной пандемии.

Четвёртая промышленная революция дала действительно революционный взрыв новых технологий. Особенно это касается разновидностей использования Интернета (Интернет вещей, Интернет тела, Интернет всего), криптовалюты и блокчейна, квантовых вычислений, 5G.

Любая новая прорывная технология используется различными субъектами в тройном назначении:

Первое. Государством и обществом – для социального и экономического развития;

Второе. Военными структурами, правоохранительными органами и спецслужбами – для повышения эффективности боевого потенциала армии и флота, обеспечения общественной и государственной безопасности;

Третье. Криминальными и террористическими структурами – для повышения незаконных прибылей и нанесения ущерба государству, обществу и личности.

Казалось бы, в одночасье целые отрасли перешли на удаленные модели работы. Виртуальная среда стала самым предпочтительным вариантом для людей, чтобы продолжать работать, учиться и общаться с близкими. По мере того, как люди генерируют, получают доступ и обмениваются большим количеством данных удаленно через облачные приложения, количество слепых зон безопасности увеличивается.

Новые технологии помогают управлять рисками и уменьшать вред от подобных угроз. Но этотпрогресс зависит от безопасной, надежной и уважающей права цифровой инфраструктуры, которая будет устойчивой и открытой для всех. Киберпространство стало гораздо большим, чем просто сфера современной человеческой продуктивности, оно всё в большей степени – область конфликта. Как правительства, так и злоумышленники постоянно совершенствуют свои методы нацеливания на противников с помощью наступательных инструментов, подрывающих коллективное доверие и безопасность.

Несмотря на достижения и инвестиции в киберзащиту, а также международные соглашения, направленные на обуздание безрассудного поведения в Интернете, конфликты в киберпространстве продолжают нарастать. Поэтому необходимо сделать гораздо больше, чем делается сегодня для повышения стабильности и безопасности в Интернете.

В ближайшем будущем правительства, корпорации и отдельные лица могут потерять способность эффективно хра-

нить свои секреты и личную информацию в безопасности, способность обеспечивать безопасные и точные демократические избирательные процессы, а также способность контролировать или отслеживать огромные объемы информации, которые постоянно проходят сквозь киберпространство.

Сфера криптоанализа находится на пути к тому, чтобы постоянно превосходить достижения в области криптологии, если только не начнут происходить математические открытия, которые позволят применять более сложные алгоритмы к процессу шифрования.

По мнению многих ведущих экспертов в сфере IT-технологий, будущее киберпространства выглядит довольно мрачным. Последние два десятилетия мы стали свидетелями распространения наступательных инструментов и операций в киберпространстве со стороны государственных и негосударственных субъектов.

Организованные преступные группы и сообщества широко используют технологии для извлечения прибыли и подрывных атак. Кибероружие, наступательные инструменты и концепции атак, разработанные одним государством, могут быть повторно использованы другими государствами, что ведёт к гонке кибернетических вооружений.

Киберугрозы стали гибридными, поскольку все более разнообразен состав злоумышленников, которые комбинируют различные методы и режимы работы против большего чис-

ла целей, создавая ситуацию неоднозначности. Цифровая трансформация, ускоренная пандемией Covid-19, экспоненциально расширила возможности и поверхность атак, создав еще больше уязвимостей.

В результате киберугрозы становятся все более системными. Такое быстрое, массовое и неконтролируемое распространение атак угрожает безопасности и стабильности самого киберпространства. Но угроза выходит за его рамки. Последствия – умышленные или непреднамеренные – могут быть серьезными, потенциально нарушая стабильность обществ, которые стали сильно зависимыми от цифровых данных и технологий.

Мы полагаемся на цифровые технологии и данные для решения сложных задач, с которыми мы сталкиваемся в области нашей коллективной безопасности, в том числе пандемии или изменении климата. Волна атак программ-вымогателей, поразивших больницы на фоне пандемии, наглядно иллюстрирует эти проблемы. Такие нападения угрожают международному миру и глобальной безопасности.

Тем не менее, несмотря на разрушительные атаки в глобальном масштабе, восприятие этого системного риска, похоже, не превалирует. Киберпространство, прежде всего, рассматривается государствами как поле стратегической конкуренцииконфронтации. Учитывая обострение геополитической напряженности между великими державами, у стран нет стимула регулировать кибершпионаж или отказы-

ваться от своих наступательных возможностей.

Международные дискуссии о нормах ответственного поведения и применении международного права в киберпространстве, безусловно, поощряли сдержанность, но разнообразие и противоречивость диалогов и процессов, похоже, зашли в тупик. Государства изо всех сил пытаются сдерживать вредоносное поведение, сохраняя при этом свои собственные пределы маневренности в киберпространстве.

Говоря о международном сотрудничестве, надо понимать, что практически невозможно просто выработать мирный договор, собрав глав государств за столом из красного дерева, чтобы нарисовать линии на карте. Границы киберпространства неуловимы, инфраструктура или поле битвы в значительной степени принадлежит частным компаниям, и природа угрозы меняется так же быстро, как мы разрабатываем правила.

Атрибуция атак в киберпространстве является сложной и неопределенной. Надлежащий ответ может оказаться сложной задачей, поскольку большинство атак либо неоднозначны, мотивированы разведывательными данными, либо находятся чуть ниже порога того, что может вызвать контрмеры в соответствии с международным правом. Кроме того, многие атаки совершаются негосударственными субъектами, которые часто действуют совершенно безнаказанно из-за недостаточного международного сотрудничества в реализации законов о киберпреступности.

Учитывая эти недостатки, мировому сообществу необходимо сосредоточиться на более сильной защите с участием всех заинтересованных сторон для устранения этого системного риска. Правительства, научные круги, гражданское общество и частный сектор должны тесно сотрудничать, чтобы способствовать наращиванию потенциала, укреплять безопасность цифровых продуктов, обучать персонал, разрабатывать значимые стратегии и политику кибербезопасности, а также улучшать сотрудничество в области анализа угроз и реагирования на инциденты.

Государства также должны инвестировать в образование и исследования, чтобы глубже понять уязвимости и стратегические зависимости, чтобы лучше предвидеть киберугрозы и киберрискии управлять ими.

Елена Ларина, Владимир Овчинский

Глава 1. Многоликий Интернет… с криминальным шлейфом

1.1. Интернет вещей

Интернет вещей (англ. Internet of Things, IoT) в совокупности с Искусственным интеллектом (ИИ), Большими данными (БД), робототехникой и блокчейн-технологией составляют суть новой промышленной революции.

Подключение большего количества «вещей» к Интернету потенциально может повысить эффективность, поднять производительность, снизить количество отходов, подстегнуть экономический рост. По данным исследования Глобального института McKinsey, к 2025 году полностью интегрированный IoT позволит ежегодно увеличивать размер глобальной экономики на сумму до $ 11 трлн.

Китайские молочные фермы, например, уже подключают стада к интернету. Коровы носят ошейники с беспроводными сенсорами. Эта информация затем используется для улучшения производства молока, что помогает фермерам зарабатывать дополнительные $ 420 с каждой коровы в год и увеличивать общую годовую прибыль на 50 %.

Один из руководителей китайского Huawei Technologies

Кен Ху считает, что для нормальной работы подключенных к Интернету энергосетей, «умных» роботов и других машин понадобятся сети нового поколения, которые будут работать быстрее и обладать еще большей мощностью.

Сети завтрашнего дня должны быть автоматизированными, самооптимизируемыми и самовосстанавливающимися. ИИ позволит поставить базовые сетевые функции на автопилот, а простые экономические соображения сделают это необходимостью. Как только Интернет вещей начнет осуществлять миллиарды подключений автомобилей, поездов, заводов и больниц, операционные затраты могут взлететь до небес, если сети не будут функционировать с минимальным вмешательством человека.

Чтобы IoT стал реальностью, властям надо будет поддержать развитие передовых сетей, способных передавать данные в более крупных объемах и гораздо быстрее. Частотный диапазон для беспроводной связи (радиоволны, с помощью которых данные невидимо перемещаются от и к подключенным устройствам) будет основой для множества цифровых услуг.

Согласно прогнозам Business Insider, умные устройства готовы влиться в каждый сегмент рынка и сделают это к 2023 году:

– на потребительском рынке умные устройства продолжат заполнять дома. Лампочки, колонки и бытовые приборы, которые будут управляться с помощью беспроводного под-

ключения, дополнятся одеждой и обувью, для организаций умные устройства продолжат играть роль автоматизации. В офисе и на производстве останутся все те же приборы, но они станут умнее и самостоятельнее, сокращая время на работу с ними;

– правительственные организации займутся стимулированием развития «умных городов». Умные камеры слежения, городские фонари и счетчики сделают борьбу с преступностью и управление коммунальными услугами эффективнее.

Термин «Интернет вещей» впервые применен в 1999 году. Его автор – исследователь Массачусетского технологического института Кевин Эштон. Он считал, что вскоре средства радиочастотной идентификации будут широко применяться для взаимодействия физических предметов с внешним окружением. Масштабное внедрение новой технологии началось в 2009 году.

Риски Интернета вещей

Резкое повышение связанности сетей не только обеспечивает их быстродействие и является важнейшей предпосылкой для сбора и обработки больших данных, но и резко повышает риски атак со стороны преступников, террористов и иных злоумышленников.

Не будет преувеличением сказать, что ситуационная среда для преступлений необратимо изменилась. В доцифро-

вом мире мы могли четко различать уличную организованную преступность и высокотехнологичный криминал. В связанном цифровом мире даже незначительное преступление может неожиданно, в том числе и для преступников, привести к целому каскаду негативных последствий.

Под Интернетом вещей обычно понимаются устройства, за исключением компьютеров, ноутбуков и смартфонов, подключенные к Интернету и друг к другу. Устройства IoT взаимодействуют без человека и помимо человека. IoT – масштабируемая гиперсеть, состоящая из беспроводных сетей и подключенных к ним устройств различного уровня автономности с уникально идентифицируемыми точками, которые информационно взаимодействуют между собой в обоих направлениях по IP протоколам без человеческого вмешательства.

Компания Intel – общепризнанный мировой лидер в области IoT – определяет его как «связанные через беспроводные технологии интеллектуальные устройства различного масштаба – от крошечных микросхем до исполинских машин, – которые взаимодействуют друг с другом и позволяют извлечь для обработки машиночитаемые данные».

Согласно британской классификации, IoT состоит из нескольких принципиально разных, но взаимосвязанных слоев или компонентов, в том числе:

– имплантированных или подсоединенных к человеческому телу электронных устройств, передающих информацию

вовне и получающих извне команды по беспроводным сетям;

– повседневных вещей с управляющими чипами, подсоединенными беспроводными сетями к внешним серверам, в том числе, предметов одежды, обуви, бытовой техники, компонентов управления домом, включая воду, электричество, охранные системы и т. п.;

– специализированных сенсорных систем видео- и иного наблюдения, подсоединенных к оптическим и беспроводным сетям. В их число входят, прежде всего, домашние, районные, коммерческие и городские системы видеонаблюдения, сенсоры аудио и термоконтроля и т. п.;

– частично или полностью автономных транспортных средств любого назначения, управляемых подключенными к двусторонним сетям программно-аппаратными устройствами;

– частично или полностью автономных производственных систем, включающих производственных роботов, частично автоматизированные линии и т. п.;

– все виды инфраструктур любого назначения, управляемых полностью или частично автоматизированными устройствами, подключенными к Интернету;

– критических инфраструктур, под которыми понимаются особо важные для национальной безопасности гиперсети и сети, обеспечивающие функционирование государственных, военных и городских объектов и сетей.

Несмотря на все достоинства IoT технологий, людей попрежнему пугают их возможности. Согласно опросу Genalto, в Великобритании около 90 % пользователей не доверяют IoT устройствам или не знают, какие дополнительные плюсы они имеют по сравнению с традиционной бытовой техникой. При этом, согласно данным того же опроса, около 75 % британцев хотели бы приобрести бытовую технику с подключенными IoT технологиями. Это – общая тенденция. Население практически всех развитых стран мира уже давно отдает себе отчет в нарушении приватности и возрастании рисков, но при этом продолжает все более активно использовать различные гаджеты. Феномен современного мира – это знание об опасностях и рисках и при этом их полное игнорирование населением и отчасти бизнесом. Больше всего респондентов опасаются утечек данных (40 %), получения несанкционированного доступа сторонних организаций к личной жизни (19 %) и использования IoT криминалом (16 %).

Еще в 2016 г. Джеймс Клеппер – тогдашний Директор национальной разведки США – сообщил, что не может исключить «использования спецслужбами – ФБР и полицией – IoT для слежения, наблюдения, определения местоположения и сбора информации о пользователях, попавших под подозрение структур национальной безопасности».

Главные риски и опасности IoT заключены в его масштабах, тотальной связанности, темпах развёртывания и независимости от взаимодействия с людьми. IoT превращает

цифровую реальность в сплошную связанную среду, где все устройства и сети взаимодействуют между собой.

Риски в значительной степени порождены тем, что IoT устройства предназначены для повседневного пользования. Они опираются на весьма простую технологию и соответственно предусматривают лишь элементарные меры безопасности. В то же время IoT устройства с каждым годом все шире используются в критически важной национальной инфраструктуре, системах жизнеобеспечении городов и сфере медицинского обслуживания. К концу 2030 года количество активных устройств Интернета вещей превысит 25 миллиардов. Соответственно любое нарушение целостности этих систем может быть предельно опасно для общества.

Департамент Внутренней безопасности США в 2017 году выявил, что еще в 2012 году злоумышленники сумели проникнуть в систему термостатов государственного завода в Нью-Джерси, производящего ядерные компоненты, и почти пять лет находились в системе. Согласно данным компании Verizon, в 2016-2017 годах IT серверы 15 университетов США подверглись атаке со стороны собственных торговых автоматов по продаже напитков и бутербродов, расположенных в кампусах. В Великобритании за этот же период было обнаружено более 1 000 уязвимостей в IoT устройствах, содержащихся в инсулиновых помпах, дефибрилляторах и кардиостимуляторах.

В интервью журналу Vice в конце 2016 года создатель по-

исковика по IoTShodan Джон Мэтерли рассказал, что в течение года ему, используя поисковик, удалось обнаружить уязвимости и подключиться к ускорителю элементарных частиц во Франции, многомегаваттной гидроэлектростанции в Китае, англо-американской единой сети суперкомпьютеров, объединяющей министерства энергетики двух стран, АНБ и британский Центр электронной разведки. Ему удалось выяснить, что эти уязвимости существовали на объектах в течение от 6 месяцев до 2,5 лет, и службы информационной безопасности не обнаружили за этот период уязвимости и утечки.

Согласно публикации газеты Times три поисковых системы по IoT, в т. ч. Shodan, Censys и Thingful, в 2017 году обнаружили в Великобритании более 500 тыс. устройств IoT, обладающих критическими уязвимостями, которые позволяют не только получать информацию с этих устройств, но и взять их под управление. Наиболее уязвимыми в Великобритании являются оснащенные IoT камеры видеонаблюдения в частном секторе, домашние системы отопления, бытовые холодильники и гаражные ворота.

ISASA (Ассоциация аудита и контроля информационных систем) несколько лет назад провела глобальный опрос о рисках IoT среди специалистов IT Англии и Уэльса. Выяснилось следующее. 44 % отметили, что в 2016-2017 годах в их организациях уже имели место случаи нарушения безопасности с использованием IoT устройств, 85 % уверены,

что это случится в ближайшие год-полтора, а 84 % отметили, что наиболее опасными для частного бизнеса являются уязвимости, присущие только IoT устройствам.

Исследователи из Университета имени Бен-Гуриона (Израиль) нашли в 2018 году в IoT ошибки, которые можно использовать для того, чтобы управлять системой «умного полива» со стороны. Получив контроль над большим количеством дождевателей, злоумышленник может израсходовать запасы воды в целом городе. По оценкам авторов, 1355 захваченных разбрызгивателей хватит, чтобы опустошить стандартную водонапорную башню в течение часа, а резервуар объемом 400 тысяч кубических метров за ночь могут исчерпать 23866 устройств.

Наша зависимость от технологий растет намного быстрее, чем способность обеспечивать от них защиту при использовании криминалом и террористами. Соответственно, вне зависимости от стараний полиции и спецслужб количество и ущерб от киберпреступлений с использованием IoT будет в ближайшие годы неуклонно нарастать. Однако это – только часть проблемы. Вторая заключается в следующем. Известно, что чем больше устройств в сети, и чем более переплетены сети, тем выше риск случайных отказов, возникновения неисправностей, которые могут привести к веерным отключениям. Специалисты по информационной безопасности полагают, что на горизонте двадцатых годов размеры и темпы увеличения сети Интернета всего будут столь велики,

что неизбежно приведут к крупномасштабным катастрофам даже без вмешательства преступников и террористов. Это, кстати, открывает для последних дополнительные лазейки. У них возникает непреодолимый соблазн осуществить злонамеренные действия в сети, маскируя их под технические неисправности.

Производители, особенно импортеры, игнорируют ответственность перед покупателем. Например, китайский производитель игрушек никогда не будет продавать плюшевых мишек с иголками внутри, а корейский производитель автомобилей не выпустит автомобиль без тормозов. Если же на рынок поставляются плюшевые мишки с IoT или автомобили с IoT устройствами, то такая ситуация не просто вероятна, а уже имеет место в реальности. Например, из-за недостаточной информационной безопасности японских автомобилей в Великобритании в 2017 году преступной группе в составе индийских математиков и украинских программистов, действующих по заказу британских преступников, удалось перехватить управление шестью автомобилями. В результате несколько человек были убиты и получили тяжелые травмы. Автомобиль с IoT стал орудием убийства.

Существуют три ключевых триггера наращивания угроз и рисков со стороны Интернета всего в повседневной человеческой жизнедеятельности, управлении государствами и функционировании бизнеса. Первый, о чем говорилось выше, это – темпы и масштабы наращивания IoT и в целом Ин-

тернета всего. Второй – на порядок худшее, чем в корпоративном и потребительском Интернете (привычном нам Интернете), состояние с информационной безопасностью. Это относится как к программам, встроенным в девайсы IoT, так и к защите коммуникации девайсов с серверами обработки данных. Третий – это синхронизация устройств IoT со смартфонами, которые в свою очередь практически беззащитны перед хакерами, киберкриминалом и террористами. Девайсы – это распахнутые настежь для деструктивных сил ворота в IoT.

Основные направления использования Интернета вещей криминалом

Эксперты США, Великобритании и ЕС выделяют несколько основных направлений использования IoT преступниками:

– использование IoT уязвимостей для вымогательства и шантажа. Развитие атак на устройства IoT во многом напоминает историю ранних атак на классические компьютеры, серверы и гаджеты. Используются наиболее вопиющие уязвимости и для атак применяется недорогой покупной софт. Очевидно, что в ближайшее время можно ожидать появления такого неприятного явления, как вымогательское ПО, нацеленное на IoT системы – компоненты умных домов, инфраструктуру умного города, публичного транспорта, робо-

тотехнических линий и т. п. Учитывая опыт классических IT систем, атаки с использованием вредоносных программ-вымогателей, действующих через IoT, могут быть весьма прибыльными для киберпреступников;

– использование уязвимостей IoT для промышленного шпионажа и криминальной разведки. Плачевное состояние дел с информационной безопасностью IoT открыло киберпреступникам возможность использования IoT устройств как ворот в «хорошо защищенные корпоративные, муниципальные и федеральные сети».

Наибольшим уровнем уязвимости обладают системы видеонаблюдения и как это ни парадоксально системы охраны периметра предприятия. Эти уязвимости, как правило, используются для проникновения в корпоративные системы и кражи оттуда документации, интеллектуальной собственности, файлов с юридическими и бухгалтерскими документами.

Наличие многочисленных уязвимостей в IoT устройствах делает IoT сети, соединяющие эти устройства, желанной добычей для киберпреступников. Они превращают такие сети в распределенные зомби-компьютеры. Эти зомби-сетевые компьютеры используются для DDoS атак на сайты и платформы в традиционном Интернете.

– использование IoT устройств для совершения тяжких криминальных преступлений. Поскольку одной из наиболее насыщенных IoT устройствами сферой является лич-

ный транспорт, то преступники используют уязвимости IoT устройств в автомобилях для перехвата управления ими с последующим инициированием катастроф.

Главная опасность бытового IoT – это использование уязвимостей IoT для проникновения в частную жизнь граждан. Согласно создателю поисковика Shodan в 2017 году при помощи этого поисковика можно было обнаружить уязвимости у родительских видеокамер в более чем 300 тыс. британских семей, подключиться к этим камерам и наблюдать домашнюю жизнь семей и их взаимоотношения с детьми.

The New Times в 2018 году опубликовала отчет о преследованиях и домашнем насилии через устройства, подключенные к Интернету. Преследователи, или, как их еще называют, абьюзеры (эмоциональный насильник) используют их не только для слежки за своими жертвами. Они меняют коды дверей, включают и выключают свет и повышают температуру термостата до невыносимого состояния. Их цель – сделать своих жертв максимально несчастными.

Стать жертвами домашнего насилия могут любые обладатели IoT устройств. Согласно статистике McKinsey, в 2017 году в 29 млн домов в США было хотя бы одно умное устройство. По данным WomenSY, уже несколько человек, обратившихся за помощью в эту организацию по борьбе с насилием, попали в психиатрические учреждения. Их расстройства связаны с тем, что умными устройствами в их доме кто-то манипулировал. Национальная горячая линия по борьбе с

бытовым насилием сообщает: с каждым месяцем все больше людей звонят с параноидальными жалобами – кто-то управляет их домом. Люди теряют контроль над дверями, динамиками, термостатами, лампами и камерами.

IoT оказывает все более значительное влияние на бизнес. Наиболее широко используются устройства IoT в авиастроении, энергетике, химической промышленности, банковском секторе, а также автомобилестроении. По состоянию на сегодняшний день именно автомобилестроение в наибольшей мере страдает от киберпреступности, связанной с IoT. В 2015 году компания Крайслер объявила о возврате 1,4 млн автомобилей после того, как пара хакеров продемонстрировали журналу Wired, что, используя IoT устройства контроля состояния тормозов, можно удаленно взять под управление автомашины Крайслер. В 2016 году ФБР выпустило специальное предупреждение, что через IoT устройства может быть перехвачено управление траками и грузовиками девяти производителей.

Основные направления преступности с использованием IoT в ближайшей перспективе 2022–2025

Можно выделить следующие основные направления наиболее опасного использования криминалом IoT в ближне- и среднесрочной перспективе:

– использование высокотехнологичного криминала в корпоративных войнах. Согласно отчету компании Gartner за 2017 год, до 25 % будущих атак на предприятия будут осуществляться через IoT устройства. «Цифровой бизнес размывает границы между виртуальным и физическим мирами. Соответственно цифровые инциденты приводят к физическому ущербу», – заявил Д. Зумерле, директор по прогнозированию в Gartner. По его мнению, до 50 % краж интеллектуальной собственности и секретных, а также конфиденциальных данных и документов из корпоративных сетей будут осуществляться хакерами, использующими для проникновения в корпоративные сети IoT. Именно IoT устройстванаряду со смартфонами станут двумя главными воротами для преступников в защищенные корпоративные сети бизнес- структур и банков;

– использование IoT для убийств и других тяжких преступлений. В цифровой среде человек будет все чаще прибегать к использованию связанных с Интернетом имплантатов, а повседневная жизнь будет проходить в среде IoT. Уже в настоящее время более 3,6 % американцев и 1,8 % британцев, в основном имеющих кардиологические и эндокринные заболевания, носят в себе имплантаты, соединённые с Интернетом. Ежегодно доля людей с вживленными чипами возрастает как минимум на 5–7 %.

В 2017 году в Великобритании было зафиксировано два случая использования уязвимостей имплантатов для попыт-

ки убийства граждан, ими обладающих. В одном случае убийство произошло, в другом – его удалось предотвратить. Полиции Лондона и Глазго по состоянию на март 2017 года не удалось изобличить преступников, хотя у них есть неопровержимые доказательства использования IoT имплантатов для совершения убийства. В начале 2019 года CNN подтвердили, что имплантируемые сердечные устройства St. Jude Medical уязвимы к атакам хакеров. Получив к ним доступ можно разрядить батарею устройства, ввести неправильный ритм или ударить током пользователя. Подобные уникальные случаи станут гораздо более распространенными в будущем и постепенно превратятся в повседневность, вытеснив традиционные виды убийств.

В настоящее время 70 % новых продаваемых машин в ЕС и Великобритании имеют жизненно важные узлы, связанные с Интернетом – IoT устройства. С 2018 года в Великобритании начали реализовываться электронные помощники Siri, синхронизированные с системой дистанционного управления автомобилем. Можно предположить, что именно автомобили станут в ближайшем будущем оружием убийства или нанесения физических травм их водителям и пассажирам.

В 2017 году полиция города Лидса, действуя совместно со Скотланд-Ярдом, смогла раскрыть группу в составе двух программистов с Украины и трех студентов университета Лидса – граждан Великобритании, разрабатывающих софт для перехвата управления автомобилем с помощью прило-

жения к смартфону, использующего помощник Siri. Главная опасность подобных преступлений состоит в том, что по мере роста квалификации преступников, они будут все более походить на несчастные случаи и соответственно оказываться вне полицейских расследований;

– использование IoT для преступлений, связанных с подключенным государством на основе подмены реальности. В 2017 году на Давосском форуме впервые был использован термин «подключенное государство». Подключенное государство – это государство, широко использующее современные информационно-коммуникационные технологии (ИКТ) для поддержания порядка и национальной безопасности. Подключенное государство базируется на широком использовании IoT и почти всегда включает повсеместное использование биометрии, анализ данных биллинга и масштабное видеонаблюдение.

В рамках подключенного государства полиция не только активно использует данные видеонаблюдения, но и с каждым годом все больше доверяет автоматизированным системам распознавания образов на основе анализа поточного видео. Программным обеспечением систем распознавания образов являются обучаемые нейросети. В 2017 году группа информационной безопасности корпорации Google опубликовала доклад. Из него следует, что команда программистов и инженеров Google смогла найти уязвимости во всех основных наиболее эффективных системах распознавания образов, в

том числе выпущенных Google, Amazon и Apple. Удалось экспериментально установить, что, используя уязвимости в программах распознавания лиц, можно удаленно и незаметно внести корректировки в алгоритмы обучения нейросети. Более того, оказалось возможным исключить определенных лиц из процесса обучения и сделать невозможным их автоматизированное распознавание системой.

Кроме того, существуют инструменты, позволяющие добиваться от нейросетей строго определенных ошибок. Их итогом становится неправильное распознавание. Программа неточно устанавливает принадлежность и не распознает преступников и в то же время маркирует благонамеренных граждан как криминальных элементов. В рамках этого исследования была протестирована система распознавания лиц Amazon Recognition. В результате взлома программы обучения удалось сделать так, что программа среди преступников, которых ей удалось опознать, установила 28 членов Конгресса США. Эти 28 членов были поименованы как преступники, которые были замечены камерами городского наблюдения Вашингтона, Нью-Йорка за совершением преступных действий. Все это происходило, когда Конгресс был на каникулах, и узнанные конгрессмены вообще не могли попасть в поле зрения видеокамер в Вашингтоне и Нью-Йорке, поскольку пребывали в своих округах. Стоимость каждого лжеопознания составила $ 12,33.

Из приведенного примера видно, что по мере перехода

к подключенному государству и все более активному использованию автоматизированных систем анализа видеопотоков криминал может подменять реальность, делая виновных невиновными и наоборот. В ближайшие годы это, скорее всего, будет доступно лишь для небольшого числа высокопрофессиональных специалистов, однако в последующем окажется под силу квалифицированным хакерам, специализирующимся на преступлениях, связанных с IoT;

– использование IoT для создания криминальных армий. Уязвимости в безопасности IoT уже в настоящее время обнаруживаются не часто. В будущем же специалисты прогнозируют, что IoT будет доступен для хакеров даже больше, чем уязвимые смартфоны. В 2016–2017 годах была разработана вредоносная программа Mirai. Зловред автоматически распознавал и идентифицировал устройства с уязвимостями и подключал их к сети. Mirai удалось собрать и использовать в течение года в криминальных целях армию ботов из более 3 млн незащищенных IP-камер, роутеров и других устройств IoT. Армия использовалась для целенаправленных атак на банки со штаб-квартирами в США и Великобритании, а также для похищения личных данных и платежных реквизитов из розничных сетей в странах ЕС. Вполне очевидно, что с каждым годом масштабы создания криминальных бот-армий из IoT устройств будут возрастать. Поскольку атака армий, включающих миллионы устройств, крайне трудна для отражения, то данная опасность должна быть ку-

пирована на начальной стадии, иначе будет поздно.

Во второй половине двадцатых годов нынешнего века экспоненциальные темпы развития информационно-коммуникационных технологий в их сегодняшнем виде станут сами по себе создавать угрозы для национальной и глобальной безопасности. В нынешнем конфликтном, все более деструктивном мире риски неконтролируемого развития ИКТ, включая IoT, накладываются на неуклонный рост могущества небольших и даже малых – в составе пяти-семи человек – деструктивных группировок хакеров, киберкриминала и террористов. Уже сегодня небольшие группы будут способны поставить под угрозу жизнедеятельность не отдельных домов или кварталов, но мегаполисов, а возможно и различного рода критических сетей. Главная проблема состоит в том, что, по оценкам большинства «фабрик мысли», специализирующихся на высоких технологиях, например, Центра новой американской безопасности для того, чтобы полностью защитить свое киберпространство в эпоху Интернета всего Соединенным Штатам ежегодно надо тратить до 3–5 % государственного бюджета, как минимум. Covid-19 также стимулирует дальнейшие инвестиции в корпоративный сектор IoT. В условиях длительного периода низких темпов экономического роста это просто невозможно. Уже сегодня Соединенные Штаты, а также Япония и Великобритания стали крепостями, которые невозможно защитить не только от вражеских киберармий, но и от банд молодых ха-

керов и небольших киберпреступных группировок, действующих поверх границ, и игнорирующих любые государственные соглашения и договоры.

1.2. Интернет тела

Неутомимый Илон Маскв рамках проекта Neuralink планирует в благих намерениях (помочь больным и обездвиженным) провести испытания нейроинтерфейса на людях и вжить нейрочип в мозг человека уже в 2022 году. На свиньях и обезьяне он уже удачные испытания провёл. Обезьяна с чипом даже поиграла в видеоигру. А реакции свиней стали похожи на реакции человека. Видимо, конечной целью является достижение результата, когда люди станут управляемые как свиньи. А что ещё внедряют людям в мозг, сердце и другие части тела?

Со стремительным развитием микроэлектроники появилась возможность встраивать элементы, передающие информацию, в предметы гардероба (часы, кроссовки, майки и т. п.), а также широко использовать микроэлектронику в новом поколении медицинской техники, реализующей различного рода имплантаты – от чипов, контролирующих сахар в крови, до кардиостимуляторов и т. п. Устройства, подключенные к Интернету, которые человек носит на своем теле, которые проглатываются или имплантируются хирургическим путем в человеческое тело, позволяющие передавать информацию через Интернет, называют по-разному. По-английски – Internet of Bodies (IoB). На русском языке встречаются такие названия, как «Интернет людей», «Интернет те-

ла», «бодинет».

С одной стороны, развитие IoB технологий порождает огромное количество данных, связанных со здоровьем, которые могут улучшить благосостояние людей во всем мире и оказаться решающими в борьбе с пандемией Covid-19. С другой стороны, широкое распространение устройств IoB порождает принципиально новые типы угроз, связанные с возможностью осуществления киберпреступлений, вплоть до нанесения тяжелых телесных повреждений и убийств, а также целевого точечного кибертерроризма. Сейчас в мире данная угроза рассматривается как актуальная, и как на государственном уровне, так и на уровне частных компаний разрабатываются конкретные меры по противодействию ей.

В октябре 2020 года американская корпорация RAND опубликовала доклад «Бодинет: возможности, риски и управление». В этом докладе обсуждаются тенденции технологического развития IoB, описываются выгоды и риски для пользователя IoB и других заинтересованных сторон. Авторы представляют текущее состояние управления, которое применяется к устройствам IoB, и данные, которые они собирают, а также дают рекомендации, чтобы наилучшим образом сбалансировать эти возможности, риски и угрозы.

Что же такое IoB? Широкий спектр «умных» устройств, подключенных к Интернету, обещает потребителям и предприятиям повышенную производительность, удобство, эффективность и удовольствие. В рамках более широко-

го Интернета вещей (IoT) находится растущая индустрия устройств, которые контролируют человеческое тело, собирают информацию о здоровье и другую личную информацию и передают эти данные через Интернет. Эти новые технологии и собираемые ими данные называются Интернетом тела (IoB). Впервые термин использовала в 2016 году американка, профессор права и инженерии Андреа М. Матвишин.

Устройства IoB бывают различные. Некоторые уже широко используются, например, фитнес-мониторы с наручными часами или кардиостимуляторы, которые передают данные о сердце пациента непосредственно кардиологу. Другие, находящиеся в стадии разработки или недавно появившиеся на рынке, могут быть менее знакомы, например, продукты для приема внутрь, которые собирают и отправляют информацию о кишечнике человека, имплантаты микрочипов – устройств для стимуляции мозга, подключенные к Интернету.

Эти устройства имеют непосредственный доступ к организму и собирают огромное количество личных биометрических данных. Производители устройств IoB обещают обеспечить существенную пользу для здоровья и другие преимущества, но также несут серьезные риски, включая риски взлома, нарушения конфиденциальности или неисправности.

Некоторые устройства, такие как искусственная поджелудочная железа для диабетиков, могут произвести революцию

в лечении болезней, в то время как другие могут просто завышать расходы на здравоохранение с небольшим положительным влиянием на результаты.

Общепринятого определения IoB не существует.

В докладе авторы называют IoB(или экосистему IoB)

устройствами IoB вместе с программным обеспечением, которое они содержат, и данными, которые они собирают.

Устройство IoB определяется как устройство, которое:

– содержит программное обеспечение или вычислительные возможности;

– может обмениваться данными с подключенным к Интернету устройством или сетью и удовлетворяет одному или обоим из следующих условий;

– собирает персональные данные о здоровье или биометрические данные человека;

– может изменить функцию человеческого тела.

Программное обеспечение или вычислительные возможности устройства IoB могут быть простыми или сложными. Обязательно требуется подключение к Интернету через сотовую сеть или Wi-Fi, но не обязательно прямое подключение. Например, устройство может быть подключено через Bluetooth к смартфону или USB-устройству, которое обменивается данными с компьютером, подключенным к Интернет у.

Данные о здоровье, генерируемые человеком (PGHD), относятся к данным о здоровье, клинических проявлениях

или самочувствии, собираемым технологиями для записи или анализа пользователем или другим лицом. Биометрические или поведенческие данные относятся к измерениям уникальных физических или поведенческих свойств человека. Наконец, изменение функции тела относится к улучшению или модификации того, как работает тело пользователя, например, когнитивное улучшение памяти, обеспечиваемое интерфейсом мозг-компьютер.

Устройства IoB обычно, но не всегда, требуют физического соединения с телом (например, их носят, проглатывают, имплантируют или иным образом прикрепляют или внедряют в тело, временно или постоянно). Многие устройства IoB являются медицинскими устройствами. Устройства, не подключенные к Интернету, такие как обычные кардиомониторы или медицинские идентификационные браслеты, не входят в определение IoB. Имплантированные магниты (используемые участниками так называемого сообщества бодихакеров) также не связаны с приложениями для смартфонов, потому что, хотя они изменяют функциональность тела, позволяя пользователю ощущать электромагнитные колебания, устройства не содержат программного обеспечения. Некоторые устройства могут подпадать под определение IoB лишь в определенное время. Например, смартфон с подключением к Wi-Fi сам по себе не будет частью IoB. Однако после установки приложения для здоровья, которое требует подключения к телу для отслеживания пользова-

тельской информации, такой как частота сердечных сокращений или количество сделанных шагов, телефон будет считаться IoB.

Авторы доклада сосредоточились на анализе существующих и появляющихся IoB-технологий, которые, по-видимому, могут улучшить здоровье и медицинские результаты, эффективность, функции или производительность человека, но которые также могут поставить под угрозу юридические, этические права и права на конфиденциальность пользователей, либо представляют риски для личной или национальной безопасности.

Развивающийся ландшафт устройств и идей IoB тесно связан с Интернетом вещей (IoT), который также не имеет универсального определения. Тем не менее, устройства IoT имеют несколько широко признанных характеристик.

Во-первых, устройства Интернета вещей подключаются к Интернету напрямую или через локальную сеть.

Во-вторых, у них есть, по крайней мере, одна из следующих функций: способность вызывать или ощущать некоторые физические изменения, напрямую получать информацию от людей, или предоставлять информацию людям, или извлекать и хранить данные.

Наконец, IoT-устройства должны взаимодействовать, чтобы приносить преимущество пользователю. Например, лампочку можно запрограммировать на включение в сумерках без подключения к сети. Она становится частью Интернета

вещей только тогда, когда она подключена к другому устройству Интернета вещей, например, к смартфону, что позволяет пользователю включать свет, не находясь дома.

Согласно определениям авторов доклада, любое устройство IoB является устройством IoT. Определение IoB включает в себя технологии из того, что часто называют Интернетом вещей в сфере здравоохранения, хотя не каждое устройство IoB в сфере здравоохранения можно считать устройством IoB. Системы роботизированной хирургии, устройства, используемые для лечения, такие как интеллектуальные аппараты ИВЛ, являются частью экосистемы IoB, поскольку они собирают информацию о пользователях и/или изменяют функции организма. Однако «умный» холодильник больницы, используемый для хранения вакцин, который может быть подключен к сети и предупреждать персонал, если запасы заканчиваются, не является устройством IoB, т. к. он не соответствует определению.

Трансгуманизм, бодихакинг, биохакинг и многое другое

IoB связан с несколькими направлениями за пределами формального здравоохранения, ориентированными на интеграцию человеческого тела с технологиями. Авторы доклада рассматривают некоторые из этих концепций, хотя между ними есть много общего и взаимозаменяемого.

Трансгуманизм – это мировоззрение и политическое движение, выступающее за трансцендентность человечества за пределами нынешних человеческих возможностей. Трансгуманисты хотят использовать технологии, такие как искусственные органы и другие методы, чтобы остановить старение и добиться «радикального продления жизни». Трансгуманисты также могут стремиться противостоять болезням, повышать свой интеллект или ноотропы (вещества, которые могут улучшить когнитивные функции).

Бодихакеры, биохакеры и киборги, которым нравится экспериментировать с улучшением своего тела, часто называют себя гриндерами. Они могут идентифицировать себя как трансгуманисты, а могут и не идентифицировать.

Эти термины часто меняются местами в обычном использовании, но некоторые действительно различают их. Бодихакинг обычно относится к модификации тела для улучшения физических или когнитивных способностей. Иногда бодихакинг носит чисто эстетический характер. Например, хакеры вживляют себе рога в голову и светодиодные фонари под кожу.

Другие манипуляции, такие как имплантация микрочипов RFID (англ. Radio Frequency IDentification, радиочастотная идентификация – прим. авторов) в руку, позволяют пользователям открывать двери, оплачивать поездки в общественном транспорте, хранить контактную информацию для экстренных случаев или совершать покупки одним

движением руки. Известен случай, когда бодихакер удалил RFID-микрочип из брелка своего автомобиля и имплантировал его себе в руку. Несколько бодихакеров имплантировали устройство, представляющее собой комбинированный беспроводной маршрутизатор и жесткий диск, которое можно использовать в качестве узла в беспроводной ячеистой сети. Иногда бодихакинг носит медицинский характер, например протезирование на 3D-принтере или искусственные поджелудочные железы.

Киборги или кибернетические организмы – это люди, которые использовали устройства для улучшения интеллекта или чувств. Нил Харбиссон, дальтоник, который может «слышать» цвет через антенну, имплантированную в его голову, играющую разные мелодии для разных цветов или длин волн света, признан первым человеком, которого правительство официально признало киборгом, поскольку ему разрешено иметь фотографию в паспорте с имплантатом.

Поскольку IoB – это обширная область, которая пересекается с самостоятельной модификацией тела, потребительскими товарами и медицинским обслуживанием, понимание его преимуществ и рисков имеет решающее значение.

IoB технологии: будущие тенденции

Развитие интернет-технологий и возможностей подключения позволит большему количеству устройств IoB и IoT

подключаться друг к другу с более высокой скоростью.

Сеть мобильной связи пятого поколения 5G может поддерживать около 1 млн устройств на квадратный фут по сравнению с предыдущей сетью 4G, которая может поддерживать около 4 тыс. устройств на той же площади. Ожидается, что Wi-Fi 6, новое поколение технологии Wi-Fi, улучшит возможности подключения, позволив еще большему количеству устройств одновременно передавать данные и взаимодействовать с маршрутизаторами. Спутниковый Интернет разрабатывается для повышения доступности Интернета, в том числе в удаленных районах, путем вывода тысяч спутников на низкую околоземную орбиту.

Некоторые разрабатываемые устройства, такие как контактные линзы с дополненной реальностью или прямой интерфейс мозг-компьютер, могут значительно изменить социальную жизнь, позволяя записывать и воспроизводить все взаимодействия человека. Нейроустройства для чтения мозга и передачи сигналов уже представлены на рынке, но улучшенные технологические интерфейсы мозг-компьютер могут помочь улучшить познание, память и контроль. Чтение и запись мозга, в конечном счете, могут быть использованы для воздействия на мысли людей в доброжелательных или злонамеренных целях.

Оценка рисков IoB

Компьютерное программное обеспечение по своей природе уязвимо для непреднамеренных ошибок или злонамеренных действий. Слабые места в коде могут быть использованы для кражи информации, собираемой устройством, или манипулировании ею, нарушения его работы или иного поведения, вызывающего непредвиденное или непреднамеренное поведение.

Технологии IoB страдают от тех же направлений атак, что и другие IoT и вычислительные устройства, но устройства IoB имеют повышенные риски в результате слияния нескольких характеристик, включая связь с организмом, тип и объем собираемой информации, а также то, как информация может быть использована.

Риски глобальной, национальной и личной безопасности

В 2018 году фитнес-компания Strava опубликовала подробную геолокационную информацию о маршрутах передвижений своих пользователей. Министерство обороны поощряло устройства для отслеживания состояния здоровья в целях борьбы с эпидемией ожирения и провело пилотную программу, в рамках которой фитнес-трекеры получили бо-

лее 2000 солдат в 2013 году и 20 000 солдат в 2015 году. Карты, выпущенные Strava, были настолько подробными и всеобъемлющими, что потенциально раскрывали скрытые военные базы и лагери американского военного и гражданского персонала, а также образ жизни военнослужащих. После инцидента военные изменили свою политику и больше не разрешают использование фитнес-трекеров.

Это всего лишь один пример того, как бурный рост инноваций и внедрение устройств IoB может представлять угрозу глобальной и национальной безопасности. Некоторые из этих рисков можно предвидеть. Например, врачи рассматривали возможность того, что для убийства вице-президента США Дика Чейни можно было использовать его кардиостимулятор. Оригинальный кардиостимулятор Чейни был оснащен функцией беспроводного мониторинга, которая потенциально могла быть взломана. В 2007 году устройство Чейни было заменено устройством без подключения к интернету.

Возможности подключения устройств к Интернету постоянно развиваются по своему характеру и качеству, и в дальнейшем они будут обеспечиваться такими коммуникационными технологиями, как 5G, Wi-Fi следующего поколения и спутниковый Интернет. Но системы связи, скорее всего, станут мишенью для злоумышленников и хакеров-преступников. Уже было показано, что у новых протоколов Wi-Fi есть недостатки в безопасности; возникли опасения по поводу 5G, особенно с учетом доминирования китайских по-

ставщиков в поставках оборудования и услуг во всем мире; а растущие программы противодействия в космосе могут поставить под угрозу спутниковые системы.

Риски кибербезопасности

Риски кибербезопасности часто группируются в три категории: по конфиденциальности, целостности и доступности.

Конфиденциальность означает, что данные видны только уполномоченным лицам; целостность означает, что собранные данные не были подделаны; а доступность гарантирует, что данные будут доступны тогда и там, где они необходимы. По состоянию на начало 2019 года Управлению по контролю за продуктами и лекарствами США (FDA) не было известно о каких-либо травмах или смертельных случаях в результате злонамеренной атаки или компрометации подключенных медицинских устройств. Однако уязвимости в этих устройствах могут случайно вызвать физический ущерб или использоваться злонамеренно для причинения вреда или смерти. Например, в имплантируемых дефибрилляторах и инсулиновых помпах существуют две хорошо известные уязвимости медицинских устройств, вызванные плохо реализованными протоколами связи между устройством и системами удаленного мониторинга. Уязвимость была обнаружена в программном обеспечении беспроводной связи обычного имплантируемого кардиовертера-дефибриллятора. Эта

уязвимость может позволить злоумышленнику перехватить обмен данными между имплантированным устройством и устройствами клинического программирования или домашними машинами для мониторинга таким образом, чтобы можно было манипулировать данными или вводить ложные (вредоносные) команды в имплантированное устройство.

Физическое устройство, имплантированное или прикрепленное к телу, будет беспроводным образом подключаться к устройству мониторинга, например, смартфону, которое затем будет передавать информацию в облачную службу. Затем данные становятся доступными для внешней стороны, такой как производитель устройства или практикующий врач. Это сочетание аппаратного и программного обеспечения, физических и логических каналов связи и организационных границ вводит множество уровней сложности, каждый из которых подвержен сбоям, ухудшению качества, компрометации и атакам.

Были предприняты попытки каталогизировать уязвимости, обнаруженные в медицинских устройствах. ICSCERT (Группа по обеспечению готовности к кибербезопасности промышленных систем управления), подразделение Министерства внутренней безопасности США, выпускает предупреждения об угрозах для медицинских устройств. Medcrypt, некоммерческая организация в области здравоохранения, ведет онлайн-документ, в котором перечислены все эти рекомендации. По состоянию на июль 2019 года она

задокументировала 144 уникальные уязвимости, обнаруженные с 2013 года. Причем количество уязвимостей растет.

Из уязвимостей, обнаруженных в этих устройствах, большинство – 65 % – связаны с аутентификацией пользователя и дефектами кода. Недостатки аутентификации пользователей могут позволить неавторизованным пользователям получать доступ и, например, нарушать конфиденциальность устройства. Дефекты кода относятся к недостаткам программного обеспечения, которые могут позволить злоумышленнику нарушить конфиденциальность, целостность или доступность системы. Хакер может заставить устройство IoB обмениваться данными с неавторизованными пользователями, манипулировать данными так, чтобы устройство работало некорректно, или просто заставить устройство перестать работать.

В дополнение к кибербезопасности самих устройств, репозитории, в которых хранятся пользовательские данные, также должны иметь достаточную защиту и средства контроля безопасности. Также необходимы важные компромиссы между безопасностью и удобством использования для устройств IoB. Рассмотрим, например, подключенную инсулиновую помпу. Лучшие практики безопасности предполагают, что доступ к устройству будет ограничен только теми, у кого есть надлежащие полномочия на выпуск или изменение инъекций, что часто делается с помощью имен пользователей и паролей или с помощью биометрического входа в

систему. Однако у пациента с инсулиновым шоком, скорее всего, не будет времени или возможности для ввода своих учетных данных в устройство.

Риски, связанные с данными и конфиденциальностью

Устройства IoB собирают и хранят сугубо личные данные, возможно, более личные, чем любой другой тип пользовательской информации, поэтому существует множество рисков для конфиденциальности. Информация о местонахождении пользователей, функциях их организма, о том, что они видят, слышат и даже думают, может быть записана и сохранена. Есть много нерешенных вопросов о том, кто имеет право использовать данные, собранные устройствами IoB, и каким образом.

Сбор данных может поставить под угрозу конфиденциальность пользователей IoB, если не будут приняты меры защиты от неправомерного использования. Сам процесс сбора, включая то, какие данные собираются, как часто, было ли получено информированное согласие (особенно в уязвимых группах населения, таких как несовершеннолетние или заключенные) и то, может ли пользователь остановить сбор данных или перепродажу в любое время, может представлять неотъемлемый риск для конфиденциальности. Потребители IoB, похоже, согласились с необходимостью предо-

ставлять свои данные разработчикам или другим лицам для использования устройства IoB. Однако неясно, получили ли потребители полное представление о том, как их данные собираются и могут быть использованы.

Есть также опасения по поводу долговечности данных, т. е. результаты набора для генетического тестирования или использование определенного медицинского устройства IoB могут идентифицировать кого-либо как носителя генетического заболевания, которое может быть передано его или ее детям, что в один прекрасный день может привести к тому, что этим детям будет отказано в определенной страховке или других льготах. Наконец, еще нет правовых норм о том, кому принадлежат данные, генерируемые любым данным устройством IoB, – пользователю, производителю, поставщику медицинских услуг? Право собственности на данные было давней проблемой в сфере здравоохранения. Специалисты, которые регулируют продажу пользовательской информации сторонним брокерам данных или регулируют работу брокеров данных, только появляются, если они вообще существуют.

Свобода от IoB

По мере того, как IoB становится всё более распространенным, может возрастать физическое или психологическое давление на тех, кто хочет жить своей жизнью с минималь-

ной зависимостью от этих устройств или взаимодействием с ними. Некоторые технологии IoB могут собирать потенциально конфиденциальную информацию помимо самого владельца. Например, устройства дополненной реальности или «умные» слуховые имплантаты предназначены для записи видео и звука. Это может вызвать беспокойство по поводу конфиденциальности у лиц, которых видят или слышат устройства, но которые не дали согласия на сбор их изображений или голосов. Одним из примеров этого явления была реакция на систему дополненной реальности Google Glass, которая вызвала общественный резонанс, что ярко было проиллюстрировано в движении «Остановить киборгов». Использование систем распознавания лиц правоохранительными органами привело к критике по поводу предвзятости систем, а также того, что они используются для классификации людей без их согласия и с ограниченным пониманием, как будет использоваться информация. Аналогичная критика относится к IoB с камерами и другими инструментами, которые можно использовать для записи или идентификации людей.

Хотя значки сотрудников, используемые для доступа к рабочему месту, будут считаться устройствами IoB, существует различие между мониторингом с пассивной обратной связью (например, считыватель бейджей издает звуковой сигнал, и дверь здания открывается, чтобы разрешить вход) и мониторингом с обратной связью, которая является се-

тевой (например, устройство постоянно отслеживает местонахождение пользователя). Amazon запатентовала технологию браслета, который может отслеживать поведение сотрудников и вибрировать, чтобы подтолкнуть их к повышению производительности. Другие технологии стремятся определить, когда работники хотят спать или отвлекаются от работы. Исследователи создают носимые устройства, которые, как утверждается, отслеживают производительность сотрудника на рабочем месте (например, количество времени, проведенное на работе, перерывы в работе, физическая активность и уровень сна) с точностью около 80 %. Эти возможности могут принести пользу работодателям и сделать сотрудников более управляемыми и эффективными на основе данных, но они могут оттолкнуть работников и нанести ущерб, если персонал считает их навязчивыми и ненужными. Наиболее вероятно, что насильственное внедрение технологии IoB произойдет в системе уголовного правосудия. Суды, тюрьмы или отделения по условно-досрочному освобождению могут оказывать давление или требовать от людей использования устройств IoB.

Перспективы устранения рисков

В докладе исследуется сложная и развивающаяся экосистема IoB, а такжеопределены различные потенциальные преимущества и риски. Множество государственных и него-

сударственных заинтересованных сторон играют свою роль в этой экосистеме, и каждая заинтересованная сторона может предпринять конструктивные шаги по устранению областей риска. Если эти риски не будут должным образом устранены, медицинские и другие преимущества IoB не будут полностью реализованы.

Содействие национальной безопасности

Устройства IoB собирают конфиденциальную личную информацию, которая может быть использована иностранными противниками, например, для ведения шпионажа. Конгресс и исполнительная власть играют особую роль в защите от подобных рисков.

Если бы события с участием Strava или вице-президента Д. Чейни произошли иначе, последствия могли бы быть огромными. Правительственные ведомства могут принять эти инциденты как уроки, извлеченные из рисков, связанных с IoB, и разработать соответствующие меры реагирования, как это сделало Министерство обороны США. Например, руководство по использованию IoB может быть разработано для высокопоставленных чиновников.

Повышение кибербезопасности

Все сетевые технологии сопряжены с риском кибербез-

опасности, но чувствительность информации IoB и потенциальные медицинские последствия нарушения или манипулирования IoB вызывают серьезную озабоченность. Правительствам необходимо подумать о том, как реализовать подход к управлению рисками, который устанавливает передовые практики и стандарты кибербезопасности для всего спектра продуктов IoB.

Поставщики медицинских услуг должны учитывать угрозы кибербезопасности, когда они рекомендуют или используют IoB. Для начала медицинские сообщества должны продолжать использовать опыт в области кибербезопасности – например, применяя опубликованные руководящие принципы, которые советуют, как создатькадровые киберресурсы здравоохранения.

Провайдеры также могут пообещать соблюдать Клятву Гиппократа для подключенных медицинских устройств, написанную массовой организацией I Am The Cavalry, которая побуждает медицинских работников и заинтересованные стороны осознавать важность кибербезопасности для пациентов. Точно так же разработчики IoB должны более внимательно относиться к кибербезопасности – например, следуя рекомендациям по кибербезопасности (даже если устройство не является медицинским) и интегрируя соображения кибербезопасности и конфиденциальности с самого начала разработки продукта.

Обеспечение конфиденциальности

Чтобы устранить риски для конфиденциальности от устройств IoB, следует рассмотреть возможность установления государственных стандартов прозрачности и защиты для данных, которые с них собираются. В нынешнем виде потребители имеют ограниченные возможности, чтобы определить, кто хранит данные об их здоровье и как эти данные используются. Поэтому в качестве отправной точки для регулирования государственные органы могут предпринять шаги пообеспечению большей прозрачности методов сбора данных.

Повышение осведомлённости

Быстрое развитие IoB создало среду, в которой пользовательские функции могут непреднамеренно использовать IoB, а также существует путаница и отсутствие ясности в отношении его возможностей. Многие технологии IoB еще неподтверждены клинической доказательной базой. Заинтересованным сторонам необходимо исследовать и распространять информацию о реальных преимуществах IoB. Есть также возможности повысить осведомленность об этических последствиях применения IoB, например, за счет дополнительного финансирования исследований, связанных со сбо-

ром данных.

Разработчики IoB могут более подробно рассказывать потребителям о рисках кибербезопасности и методах использования конфиденциальных данных, связанных с их продуктами. Наконец, пациенты и пользователи должны осознавать риски, связанные с принятием решений об использовании таких устройств.

По мере развития интеллектуальных устройств в здравоохранении грань между человеком и машиной стирается, что вызывает новые опасения по поводу безопасности носителей IoB устройств и прав на неприкосновенность частной жизни.

Устройства IoB могут быть подвержены тем же недостаткам безопасности, что и IoT устройства или любая другая технология, которая хранит информацию в облаке. Но, учитывая характер IoB устройств и собираемых ими данных, ставки особенно высоки. Уязвимости могут позволить неавторизованным сторонам взломать устройства, что приведет к утечке частной информации, подделке данных или блокировке доступа пользователей к их учетным записям.

В случае некоторых имплантированных медицинских IoB устройств хакеры потенциально могут манипулировать ими, чтобы причинить телесные повреждения или даже смерть. Можно имплантировать в глаз искусственный хрусталик для коррекции зрения, но такие линзы также могут однажды начать записывать все, что вы видите. Электронные таблетки с Bluetooth разрабатываются для мониторинга внутренней ра-

боты тела, но в итоге они могут транслировать, что человек ел, или принимал ли наркотики. Можно восстановить слух с помощью имплантата, но нужно иметь в виду, что он также имеет возможность записывать данные об окружающей звуковой среде. IoB проблематичен по своей конструкции и вызывает серьезные опасения в отношении кибербезопасности, конфиденциальности и защиты конфиденциальных данных. Наличие устройства, непосредственно прикрепленного к телу, увеличивает потенциальный ущерб, который может нанести взлом или преднамеренный сбой.

Хотя убийство с помощью кардиостимулятора может показаться надуманным, тем не менее, создаются прецеденты для использования данных Интернета тела в уголовных расследованиях. Например, медицинские данные кардиостимулятора использовались для предъявления обвинений в поджоге и мошенничестве со страховкой человеку, который предположительно сжег свой дом в 2016 году. Мужчина утверждал, что пожар начался сам по себе, и что он собрал свои вещи и выбросил их из окна спальни, чтобы спастись. Но кардиолог пришел к выводу, что показания кардиостимулятора, включая частоту сердечных сокращений и сердечные ритмы, делали это маловероятным, учитывая состояние сердца человека. Ссылаясь на нарушение неприкосновенности частной жизни своего клиента, адвокат этого человека потребовал исключить доказательства, но судья постановил разрешить использование данных в суде.

Исследования показывают, что IoB-технологии используются не только в медицине, но и в других сферах, например, в военной. Знаменитое агентство DARPA – Управление перспективных исследовательских проектов Минобороны США – в 2019 году получило из бюджета $65 млн на программу по созданию интерфейса «человек-компьютер», предполагающего имплантацию специального устройства прямо в голову. По замыслу авторов, чип будет стимулировать разные отделы головного мозга, чтобы повысить те или иные характеристики солдата (Илон Маск идёт по пути, проторенному военными). В Пентагоне рассчитывают со временем дать бойцам сверхчувствительность и ускорить их реакцию. Над проектом работают сразу шесть исследовательских групп. Четыре отвечают за улучшение зрения, две – за слух. И это понятно: в современной войне победит тот, кто первым увидит или услышит противника. Мозг военнослужащего собираются напрямую связать с компьютерной сетью, из которой солдаты смогут в режиме реального времени получать информацию о происходящем на поле боя, не отвлекаясь на тактический планшет или рацию.

Таким образом, любая вновь созданная технология не только открывает новые возможности для человечества, но и содержит определенные, иногда значительные, риски и угрозы, в какой бы области эта технология не использовалась.

1.3. Интернет всего

Развитие глобальной сети привело к появлению виртуальных соединений, повсеместно проникающих сквозь объекты и действия реального мира. Сегодня все может быть связано со всем, создавая новую распределенную экосистему, выходящую за рамки уже знакомой концепции «Интернета вещей (IoT)». Для описания этой динамично меняющейся экосистемы был придуман специальный термин – «Интернет всего (Internet of Everything – IoE)».

Технологическое и социальное содержание Интернета всего

По определению компании Cisco: Интернет всего (IoE) объединяет людей, процессы, данные и вещи, чтобы сделать сетевые соединения более актуальными и ценными, чем когда-либо прежде, превращая информацию в действия, которые создают новыйпотенциал, обогащают опыт и создают беспрецедентные экономические возможности для бизнеса, отдельных лиц и стран.

Технически IoE относится к миллиардам устройств и потребительских товаров, подключенных к Интернету в интеллектуальной сетевой среде. По сути, это философия, описывающая мир, в котором миллиарды датчиков имплантиро-

ваны в миллиарды устройств, машин и обычных объектов, что дает им расширенные сетевые возможности и, таким образом, делает их умнее. В соответствии с этой философией наше технологическое будущее зависит от различных типов приборов, устройств и вещей, подключенных к глобальному Интернету.

Термин «Интернет всего» ввел в оборот футуролог компании Cisco Дэйв Эвансеще в 2012 году. Ценность Интернета всего заключается не в объеме информации, которая есть в Сети, а в объеме информации, которой обмениваются между собой с какой-то целью. В Интернете всего ценностью являются не сами вещи, а связи между ними. Иногда исследователи ставят знак равенства между Интернетом вещей (IoT) и Интернетом всего (IoE). Однако разница между ними есть, она заключается в разумной связи.

Интернет вещей – это сеть физических объектов, которые имеют встроенные технологии, позволяющие осуществлять взаимодействие с внешней средой, передавать сведения о своем состоянии и принимать данные извне. Возможности IoT не ограничиваются только подключением устройств, но и позволяют определять, анализировать, обрабатывать или передавать данные, генерируемые этими устройствами. Они используются для сбора информации, отправки информации или того и другого, создавая таким образом сеть физических вещей. Собранные данные отправляются в облако, где шлюзы Интернета вещей или другие периферийные устрой-

ства анализируют эти данные. Системы IoT могут функционировать и контролировать себя без какого-либо вмешательства человека. IoE объединяет людей, процессы, данные и вещи и объединяет их в сеть. Другими словами, Интернет всего можно определить как расширенную версию Интернета вещей или его новую фазу.

Даже самый беглый взгляд показывает, что Интернет всего сохраняет преемственность с более ранними стадиями развития глобальной сети. В нём, естественно, присутствуют и люди, для которых сеть и была создана, и вещи, которые представляют сейчас большую часть её населения. И добавляются две новых категории. Это данные и процессы. Плюс к изначальным связям человека-с-человеком (Peopletopeople, P2P) добавляются ещё коммуникации человека-с-машинами (Peopletomachine, P2M) и машин-с-машинами (Machinetomachine M2M). Но всё же главное – это данные и процессы.

Говоря о составляющих IoE, можно выделить четыре ключевых компонента:

Люди. Люди одновременно служат источниками данных и ключевыми бенефициарами IoE. Люди будут подключаться к Интернету самыми разными способами. Они смогут генерировать данные и взаимодействовать с устройствами не только через мобильные устройства/планшеты, персональные компьютеры и социальные сети, но и через датчики, размещенные на коже или в теле человека, а также вши-

тые в одежду или носимые на теле, что обеспечит сбор жизненно важных показателей человека. Таким образом, люди сами станут узлами в интернете. В настоящее время индустрия устройств, которые управляют человеческим организмом, собирают медицинскую и другую личную информацию, а также передают эти данные через Интернет, растет в геометрической прогрессии. Эти новые технологии и собираемые ими данные называются Интернетом тела (IoB). Хорошим примером является носимый фитнес-браслет Nike, который считывает жизненные показатели человека, а также спортивная одежда и снаряжение со встроенными чипами, которые отслеживают результаты спортсменов.

Вещи. Вещи и физические элементы, такие как датчики, промышленные устройства, потребительские товары, производственное оборудование, будут подключены к интернету и/или друг к другу, плюс, получая информацию из окружающей среды, они станут более «мыслящими» и интеллектуальными. Это и есть Интернет вещей. По состоянию на 1984 год к Интернету было подключено только 1000 устройств, их количество увеличилось примерно до 1 миллиона в 1992 году. По оценкам, к 2030 году количество активных устройств Интернета вещей достигнет 25,4 миллиарда.

Данные. Данные – это источник жизненной силы любой системы IoE. Передаваясь в разных направлениях по различным сетевым «венам», они связывают все воедино и позволяют системе работать. Однако они также создают колос-

сальные проблемы с точки зрения подключения, хранения и обработки. Будущие системы IoE, вероятно, будут иметь тысячи и тысячи довольно сложных датчиков, передающих что угодно, – от цифровых значений до изображений в высоком разрешении – и все это должно быть обработано как можно быстрее, что потребует нового уровня знаний в области обработки данных и навыков работы с большими данными.

Процесс. Процессы – это ядро IoE. Они представляют собой сетевые «соединения» и потоки данных/информации в реальном времени между узлами IoE. Различные процессы, основанные на искусственном интеллекте, машинном обучении или других технологиях, обеспечивают отправку нужной информации нужному человеку в нужное время. Цель процессов – гарантировать наилучшее использование больших данных.

Область потенциальных применений IoE практически безгранична, существуют сотни возможных сценариев для каждой отрасли. Решения IoE уже сегодня развертываются во многих секторах, включая автомобилестроение, транспорт, умные дома, энергетику, коммунальные услуги, безопасность, наблюдение, общественную безопасность, финансовые услуги, розничную торговлю, здравоохранение, промышленность, складирование и дистрибуцию. Вот лишь некоторые из них.

Глобальная логистическая индустрия является идеальным кандидатом на использование IoE. С помощью IoE

улучшения технологических процессов возможны буквально везде: от складов и сортировочных комплексов до воздушных портов и станций технического обслуживания. Например, использование сенсорных матриц и программного обеспечения для управления портами на базе искусственного интеллекта в морских портах может привести к многомиллионной экономии средств – в результате оптимизации операций стыковки и погрузки/разгрузки, прогнозного обслуживания оборудования и автоматизации складских процессов.

Современное здравоохранение – это еще одна область, где внедрение правильно работающих инновационных сценариев IoE может оказать огромное влияние и спасти жизни людей. Подразделения экстренного реагирования в больницах могут быть подключены к платформам управления дорожным движением для быстрой и беспроблемной транспортировки пациентов в больницы. Аналогичным образом этот вид автоматизации может быть применен в операционных, отделениях интенсивной терапии, медицинских лабораториях и так далее.

Термин «Интернет вещей» когда-то был придуман для совещания по управлению цепочками поставок и логистике, поэтому нет абсолютно никаких сомнений в том, что его преемник IoE станет долгожданным дополнением к любой системе управления поставками будущего. Это особенно верно для особых типов цепочек поставок, связанных с определен-

ными типами грузов, – например, цепочки поставок продуктов питания, чувствительных к температуре, медикаментов и химикатов. Элементы IoE в области управления цепочками поставок помогут оптимизировать большинство процессов, минимизировать производственные издержки, выровнять спрос и предложение в полностью автоматическом режиме.

Вся парадигма IoE идеально подходит для того, чтобы вдохнуть жизнь и интеллект в дорожную инфраструктуру, поскольку различные компоненты дороги одновременно взаимодействуют друг с другом, транспортными средствами и дорожными службами. IoE позволит увеличить среднюю скорость движения, снизить количество аварий, поскольку для интеллектуального управления дорожным движением можно использовать мощные алгоритмы искусственного интеллекта. В сочетании с неуклонно растущим числом электромобилей с автопилотом и подключением к сети 5G такие реализации IoE могут стать самыми впечатляющими и эффективными проектами.

Системы умного дома – это то место, где Интернет вещей изначально начал развиваться как концепция и технология. Сегодня, когда на рынке представлены тысячи продуктов домашней автоматизации, превратить дома в экосистемы IoE проще, чем когда-либо, если имеются необходимые навыки и опыт в области IoT. В типичном американском домохозяйстве, как правило, уже есть один или два голосовых по-

мощника, умный дверной звонок, подключенный термостат и, возможно, целый комплект подключенных к «Интернету приборов и устройств». Необходимо лишь «завязать» их в единую сеть.

Организации, которые внедряют решения IoE, меняют свои процессы, чтобы использовать инновации во взаимосвязанном мире, где вещи и люди могут сотрудничать по-новому. IoE включает в себя технологические решения, которые повышают производительность, оптимизируют затраты, способствуют внедрению инноваций, укрепляют безопасность и глобальное управление ресурсами для организаций частного и государственного секторов. Решения IoE используются как в развитых, так и в развивающихся странах мира.

При наличии такого большого количества аппаратного обеспечения появление более совершенных облачных платформ и доступных датчиков Интернета всего, которые будут размещены на линиях электропередач, трубах, заборах и других важных местах современного дома, – это всего лишь вопрос времени.

Футуролог Cisco Дейв Эванс убежден, что благодаря технологиям IoE мир претерпевает большие изменения уже сейчас и изменится еще больше в будущем. В своем блоге он описывает еще несколько положительных изменений, ожидаемых им в будущем:

Лучшее снабжение продуктами питания. Датчики по всей цепочке поставок продуктов питания вместе с аналитикой

больших данных и интеллектуальными возможностями облачных сервисов помогут оптимизировать доставку продуктов питания от «фермы до стола». Датчики на поле будут объединяться с прогнозами погоды и другими данными, чтобы определять время полива и сбора урожая для каждой культуры. А датчики на самом продукте будут предупреждать продавцов и потребителей о приближении окончания сроков годности, чтобы предотвратить порчу. Все это позволит значительно сократить пищевые отходы, которые сегодня составляют около одной трети от общего мирового производства продуктов питания.

Лучшее водоснабжение. Сегодня около 30 % воды систем водоснабжения теряется из-за утечек и попадания в отходы. Всего лишь один кран или протекающая труба, капающая три раза в минуту, приводит к потере более 100 галлонов воды в год. «Умные» трубы могут значительно сократить эти отходы, обнаруживая и точно определяя места утечек, которые в противном случае оставались бы незамеченными в течение месяцев или лет.

Лучший доступ к образованию. Это – один из наиболее перспективных социальных лифтов. Вскоре время и расстояние больше не будут ограничивать доступ к привлекательному, доступному и качественному образованию. С ростом скорости соединения и снижением стоимости оборудования дистанционное обучение выйдет за рамки традиционных онлайн-классов и создает общедоступные иммерсивные (по-

гружающие в виртуальную среду), интерактивные возможности обучения в реальном времени. Этот процесс мы наблюдаем уже сейчас, когда из-за пандемии Covid-19 учащихся активно переводят на удаленное обучение.

Лучший доступ к здравоохранению. Урбанизация и рост населения создают нагрузку на ресурсы здравоохранения, особенно в сельской местности.

Вскоре женщины сбеременностью с высокими рисками смогут носить крошечную, постоянно работающую электронную «татуировку» для мониторинга состояния плода, которая будет связываться с облаком всякий раз, когда женщина находится в пределах досягаемости беспроводной сети. Возможности аналитики в облаке будут предупреждать врачей о первых признаках неприятностей и даже сообщать будущей матери, когда ей, например, нужно пить больше воды или больше отдыхать.

Дейв Эванс выделил всего четыре области, в которых IoE изменит мир. Но нет ни одной части жизни, на которую IoE бы не повлиял каким-либо образом – будь то ускорение прохождения кассы в продуктовом магазине, экономия энергии за счет умного освещения или сокращение времени ожидания переключения светофора. Интернет всего – это не серебряная пуля, которая может решить все мировые проблемы, но благодаря искре человеческих инноваций IoE может стать двигателем для лучшего будущего.

Риски и угрозы Интернета всего

Будущее IoE, на первый взгляд, кажется безоблачным. Но по мере увеличения числа устройств, подключенных к Интернету, и, следовательно, сбора большего количества данных, для их конфиденциальности возникают новые риски и угрозы. В то время, как эти устройства и сети становятся более интеллектуальными, необходимо, чтобы они также стали достаточно осведомленными для обнаружения и предотвращения любых рисков и угроз. В каких же областях Интернет всего может создать наибольшие риски?

Персональные данные пользователей. Учитывая, что в умном городе все подключено ко всему через сеть, скрыть свои данные от посторонних глаз становится крайне сложно. Возьмите, например, системы видеонаблюдения на улицах некоторых городов – они позволяют выявлять и наказывать злоумышленников. Но при этом в объективы камер попадают обычные люди, не желающие становиться объектом внимания.

Безопасность. Она связана с предыдущим моментом – информационная или физическая безопасность становится крайне важной в контексте IoE. Чем больше данных размещено в интернете, тем выше к ним интерес мошенников.

Киберугрозы. Дело в том, что вендоры (поставщики товаров) IoE-систем чаще всего собирают свои устройства

из комплектующих различных производителей. Ранее разработчики ориентировались в основном на функционал устройства, часто не уделяя надлежащего внимания аспекту безопасности. Компоненты IoE-устройств и сами системы часто не тестируются производителями, поэтому на их взлом уходят буквально минуты. После серии громких инцидентов взлома подключенных к Интернету устройств уровень безопасности новых моделей возрос. В целом, важно помнить, что чем больше подключенных устройств в мире становится, тем активнее киберпреступники, пытающиеся получить доступ к социальному обеспечению, банковским счетам и личной переписке пользователя.

Интернет всего представляет собой особую сферу изучения для правоохранительных органов и спецслужб из-за количества и разнообразия аппаратных средств, программного обеспечения и протоколов связи, которые правоохранительные органы и спецслужбы должны иметь возможность исследовать, а также с точки зрения идентификации устройств и извлечения данных, имеющих отношение к конкретной ситуации. Чаще всего для этого требуется криминалистическая экспертиза данных в реальном времени, поскольку некоторые или все соответствующие данные могут находиться в облаке, что часто требует международного сотрудничества и юридической помощи.

Кроме того, извлечение, идентификация и объединение соответствующих доказательств обычно становятся пробле-

мой больших данных, требующей от правоохранительных органов и спецслужб наличия необходимых навыков. Увеличение количества и разнообразия устройств, вероятно, приведет к значительному увеличению спроса на ресурсы для криминалистической экспертизы и расследования. Можно ожидать, что IoE еще больше усложнит атрибуцию преступлений, учитывая увеличившуюся поверхность атаки и большое количество векторов атак.

Ключевыми аспектами IoE являются идентификация, безопасность, конфиденциальность и доверие. Например, функции распознавания лица и речи в интеллектуальных устройствах станут более распространенными и будут представлять больший риск с точки зрения конфиденциальности и безопасности, как и носимые технологии, которые могут собирать данные. Как известно, чем больше данных будет собираться, агрегироваться и использовать перекрестные ссылки, тем труднее будет защитить конфиденциальность этих данных.

По мере того, как все больше объектов подключается к Интернету и создаются новые типы критически важной инфраструктуры, нужно ожидать больше целевых атак на существующие и появляющиеся инфраструктуры, включая новые формы шантажа и схем вымогательства (например, программы-вымогатели для умных автомобилей или умных домов), кражи данных, телесные повреждения и возможная смерть, а также новые типы ботнетов (скрытно установ-

ленных программ на устройствах потенциальных жертв кибер-злоумышленников).

Поскольку все больше (личных) данных хранится в облаке, можно ожидать увеличения числа атак на облачные сервисы с целью нарушить работу сервисов по экономическим или политическим мотивам, украсть/получить доступ к данным, например, при помощи программ-вымогателей, или использовать инфраструктуру для злонамеренных целей. Многогранный характер IoE требует столь же разнообразной реакции со стороны правоохранительных органов, спецслужб и структур безопасности бизнес-компаний. Помимо навыков, знаний и опыта, которые необходимы правоохранительным органам для расследования преступлений, связанных с Интернетом всего, сотрудничество и координация вместе с государственно-частным партнерствами будут играть все более важную роль. Это может включать, например, создание репозиториев (хранилищ) для сбора, сопоставления и анализа данных, полученных или восстановленных с различных устройств, в соответствии с действующими правилами конфиденциальности и защиты данных.

По мере того, как IoE получает все более широкое распространение, количество и типы ресурсов цифровой криминалистики, требуемые правоохранительными органами и спецслужбами, должны соответственно адаптироваться и расти. Отрасли, вовлеченные в создание IoE, необходимо поощрять к тому, чтобы они рассматривали безопасность как часть

процесса проектирования.

И последнее, но не менее важное: директивным органам необходимо быть в курсе последних событий в этой области, чтобы гарантировать наличие эффективных, действенных и сбалансированных законодательных и нормативных актов.

Поможет ли Интернет всего смягчить социальное и цифровое неравенство или усугубит его?

В Обзоре ЮНКТАД (Конференции ООН по торговле и развитию) «Вскочить на волну технологий. Инновации со справедливостью» 2021 года отмечено, что научно-технический прогресс и финансовый капитал вместе создают новые технико-экономические парадигмы – сращение технологий, продуктов, отраслей, инфраструктуры и институтов, которые характеризуют технологическую революцию. IoE как раз и является инструментом такого сращения. В Обзоре ЮНКТАД отмечено, что в странах, находящихся в центре новых технологических волн, стадия подъема разделяется на два этапа. Первый – этап освоения, когда технология получает применение в основных отраслях, увеличивая разрыв между работниками этих отраслей и остальными. Второй – этап широкого внедрения, которое также часто происходит неравномерно: не каждый получает немедленный доступ к благам прогресса. В результате усиливаются различия, что может

привести к напряженности в обществе.

Многое будет зависеть от того, будут ли страны закрывать разрыв, продвигаться вперед или отставать, что, в свою очередь, будет зависеть от их государственной политики.

Все технологии необходимо использовать осторожно, чтобы они помогали, а не мешали или вызывали непредвиденные побочные последствия. Технологии могут влиять на неравенство, но неравенство также может в свою очередь воздействовать на технологии, которые таким образом отражают, воспроизводят и, возможно, усиливают системную предвзятость и дискриминацию.

Люди испытывают воздействие передовых технологий как потребители товаров и услуг, в которых такие технологии воплощены. Один из наиболее важных аспектов – доступ, который можно рассматривать как сочетание наличия, доступности, информированности, приемлемости по цене и возможности эффективного использования.

Страны сталкиваются со следующими основными проблемами в усилиях по обеспечению равного доступа к преимуществам передовых технологий: Высокая бедность по доходам – многие люди в большинстве стран, в том числе и в нашей, не могут позволить себе новые товары и услуги, особенно в сельской местности. В данном случае препятствия носят не технический, а экономический и социальный характер. IoE относится именно к таким технологиям, где возникают социальные препятствия по внедрению. Цифро-

вой разрыв – многие передовые технологии, особенно IoE, рассчитаны на стабильное высокоскоростное проводное соединение с Интернетом, но почти половина населения мира по-прежнему не имеет подключения к нему. На начало 2021 года по данным Российской ассоциации электронных коммуникаций широкополосный Интернет не был доступен для каждого пятого россиянина. Около 40 процентов школ, фельдшерских пунктов и других соцобъктов ещё не подключены к Интернету. Недостаточная цифровая подготовка потребителей новых технологий тоже относится к этому комплексу проблем. Научно-технический прогресс необходим, но он же способен увековечить неравенство или создать его новые проявления в результате ограничения доступа более привилегированными группами. Это в полной мере относится и к Интернету всего.

Задача государства при внедрении IoE состоит в том, чтобы добиться получения как можно больших выгод при одновременном уменьшении вредных последствий и обеспечении всеобщего доступа.

Глава 2. Искусственный интеллект

2.1. Как развивается искусственный интеллект?

Искусственный интеллект полон противоречий. Это мощный инструмент, у которого есть потенциал для улучшения человеческого существования. В то же время он способен углубить социальный разрыв и лишить работы миллионы людей. Хотя внутренняя суть ИИ носит сугубо технический характер, люди, не являющиеся техническими специалистами, могут и должны понимать основные принципы того, как он работает, и те проблемы, которые он вызывает.

Всемирный экономический форум (ВЭФ) с 6 апреля 2021 года в рамках своей Экспертной сети организовал обсуждение проблем ИИ. Оно проводилось в разделе Стратегическая разведка ВЭФ.

Резкое увеличение финансирования ИИ в последнее десятилетие отражает прогресс в его возможностях. В науке ИИ продвигает исследования в области молекулярных открытий, понимания системной биологии человека и физики всего: от элементарных частиц до галактик. Прикладные инновации ИИ, скорее всего, улучшат медицину, сделают

транспорт более безопасным, а прогнозы погоды более точными.

Исследования ИИ также становятся все более междисциплинарными, поскольку социологи и экономисты, например, объединяют ИИ и методы статистического вывода причинно-следственных связей в целях развития своих областей. Подобные разработки необходимы для повышения доверия к использованию ИИ в ряде сфер, в которых решения или прогнозы «черного ящика» могут содержать риски и угрозы для его использования, например, в критической инфраструктуре и кибербезопасности, расширении возможностей ИИ в государственных и частных службах, а также для содействия решению проблем, связанных с обработкой конфиденциальной и личной информации.

Пандемия повлияла на количество стартапов в области ИИ в мире – оно резко снизилось: с 2199 новых компаний в 2019 году до 692 в 2020-м, что следует из отчета AI Indexreport 2021 Стэнфордского университета. Несмотря на это, частные инвестиции в сектор увеличились почти на 10 % – с $38 млрд до $42 млрд. Лидерами по объему привлеченных средств стали технологические компании в области создания при помощи технологий ИИ новых лекарств, в том числе, для борьбы с раком, а также проводящие исследования в области молекулярной медицины, отмечается в исследовании Стэнфордского университета. Эти разработки были профинансированы на сумму более $13,8 млрд, что

в 4,5 раза больше, чем в предыдущем году. За ними в списке следуют разработчики автономного транспорта ($4,5 млрд) и компании, развивающие образовательные продукты с ИИ ($4,1 млрд).

В сфере ИИ резко возросло значение этики. В последние годы количество научных статей, в которых упоминаются моральные риски ИИ, значительно увеличилось. Основными темами стали конфиденциальность, прозрачность и объяснимость, следует из отчета университета.

Первая страна по объему инвестиций – США. В 2020 году американцы вложили в отрасль $23,6 млрд – почти на 20 % больше, чем в 2019-м. Количество новых компаний за этот же период выросло со 184 до 647. Следом за Соединенными Штатами идут Китай и Индия. Эти страны в прошлом году вложили в ИИ $10 и $0,5 млрд.

Ситуация в России

В России в год пандемии вложения в ИИ сократились почти на четверть – с $26 млн в 2019-м до $18 млн в 2020 году, уточняется в AI indexreport 2021. Количество новых компаний в РФ снизилось с 12 до трех. По сумме притока частного капитала Россия занимает только 38-е место.

В 2021 году началась реализация профильного федерального проекта «Искусственный интеллект» национальной программы «Цифровая экономика России». Государ-

ственная поддержка, например, инициатив в области технологий машинного обучения превысит 18 млрд руб лей до 2024 года. Кроме того, там заложены средства на внедрение образовательных программ в вузах, и пилотных проектов по ИИ на средних и крупных предприятиях.

26 марта 2021 года Президент России Владимир Путин на заседании наблюдательного совета автономной некоммерческой организации (АНО) «Россия – страна возможностей» отметил, что амбициозные задачи по применению новейших разработок в сфере ИИ ставятся во многих сферах, начиная от ЖКХ и здравоохранения и заканчивая космосом. 29 марта 2021 года на совещании с вице-премьерами председатель Правительства РФ Михаил Мишустин отметил, что стартапы и небольшие IT-компании смогут получить гранты на развитие проектов с использованием технологий ИИ. В 2021 году на эти цели предусмотрено 1,4 млрд руб лей. Правительство утвердило Правила предоставления такой поддержки. Претендовать на гранты могут как малые предприятия, так и физические лица. Для отбора будут важны новизна разработки, эффективность предлагаемых решений, перспективность внедрения и коммерческой реализации продукта. Субсидии предусмотрены на разработку новых сервисов и решений и на акселерацию проектов (помощь в развитии проекта и выводе продукции на рынок). Также господдержку можно получить на создание открытых ИИ-библиотек – бесплатных ресурсов, на которых собраны программ-

ные коды для работы ИИ. Каждый разработчик сможет воспользоваться такими сервисами и внедрить необходимые коды в свои ИИ-проекты.

Проведением конкурсного отбора претендентов и предоставлением финансирования займётся Фонд содействия развитию малых форм предприятий в научно-технической сфере.

Совершить прорыв в области ИИ невозможно без учёта опыта других стран.

Общий мировой тренд

30 стран разработали национальные стратегии ИИ. На сегодняшний день Соединенные Штаты занимают первое место в области ИИ, но Китай бросает вызов их лидерству. Например, Китай обошел США по числу цитирований научных статей по ИИ. При отсутствии значительных политических изменений как в ЕС, так и в Соединенных Штатах, в частности, ЕС меняет свою систему регулирования на более открытую для инноваций, а Соединенные Штаты разрабатывают и финансируют более активную национальную стратегию ИИ. Вероятно, что ЕС останется позади как США, так и Китая, а Китай будет скорейшими темпами ликвидировать разрыв с Соединенными Штатами.

Подходы к ИИ в Китае, США и ЕС отражают их относительно сильные стороны – государственный контроль в Ки-

тае, голос граждан в Европе и деловую практику в Америке. Стратегия Китая, не связанная с проблемами конфиденциальности, направлена на использование обилия внутренних данных и развитие талантов в области ИИ с помощью централизованных схем и массовых вливаний денег. Нормативные акты и приоритеты Европейского Союза в отношении расходов руководствуются целью укрепления доверия граждан к технологиям на основе ИИ путем защиты конфиденциальности и устранения сбоев на национальных рынках труда. Основа американского подхода – укрепление связей между бизнесом и исследованиями, связанными с ИИ, и поиск способов финансирования базовых НИОКР.

Несмотря на усилия по внедрению инноваций в области ИИ, все эти экономики сталкиваются с проблемами. Стратегия Китая в области ИИ продолжает полагаться только на трех технологических гигантов: Baidu, Tencent и Alibaba, которые инвестируют более чем в 100 компаний, занимающихся ИИ. Ресурсы ИИ в Европе географически несбалансированы-четверть талантов в области ИИ в Европе находится в Великобритании, а еще четверть – в Германии и Франции. Серьезный риск для развития ИИ представляет Брексит. Более половины талантов в области ИИ в США – иностранцы, поэтому иммиграционная политика неизбежно станет центральным компонентом национальной стратегии ИИ.

Политика США в области ИИ

Администрация Д. Байдена унаследовала набор стратегий ИИ, которые основываются на политике администрации Б. Обамы. Национальный стратегический план исследований и разработок в области ИИ, подготовленный в 2016 и обновленный в 2019 году, устанавливал приоритеты федеральных инвестиций в исследования и разработки в области ИИ, а исполнительный указ № 13859 запустил американскую инициативу в области ИИ в 2019 году. В соответствии с Законом о Национальной инициативе в области ИИ было создано Управление Национальной инициативы в области ИИ Белого дома. Ему поручено координировать национальную стратегию искусственного интеллекта – потенциально мощный инструмент для стратегического продвижения ИИ. Бюро управления и бюджета (OMB) выпустило рекомендации, как сбалансировать регулирование ИИ таким образом, чтобы устранить риски ИИ и поддержать инновации в области ИИ. Они, в том числе, содержат рекомендации по регулированию ИИ, а также потенциальную дорожную карту для других правительств.

Закон об утверждении ассигнований на 2021 финансовый год на военную деятельность Министерства обороны (NDAA) продолжает развивать политику ИИ в оборонном и других секторах. Закон предусматривает ассигнования на

формирование Национальной целевой группы по исследованиям ИИ с целью изучения возможности создания национального исследовательского ресурса по ИИ. Он также содержит разрешение Национальному научному фонду (NSF) на создание национальных исследовательских институтов ИИ и поручение Национальному институту науки и техники NIST разработать структуру управления рисками в области ИИ. Только в 2020 году федеральное правительство потратило почти $ 1 млрд на исследования и разработки в области ИИ и объявило о выплате $ 140 млн в течение пяти лет семи научно-исследовательским институтам по проблемам ИИ, возглавляемым NSF.

Американская инициатива в области ИИ признает, что партнерские отношения с друзьями и союзниками США представляет собой ключевой источник стратегического конкурентного преимущества и определяет необходимость международного сотрудничества для создания глобальной среды, поддерживающей американские исследования и инновации в области ИИ. Цели взаимодействия включают поддержку внедрения заслуживающих доверия инноваций в области ИИ, укрепление доверия к технологиям ИИ и их внедрение в интересах экономического роста и глобальной безопасности.

Кроме того, США осуществляют усилия по развитию международного сотрудничества в области ИИ, которые включают двусторонние соглашения о сотрудничестве с Ве-

ликобританией в области исследований и разработок ИИ, участие в международных и многосторонних инициативах, таких как встреча министров науки и технологий Большой семерки, которая запустила Глобальное партнерство по ИИ.

Политика Китая в области ИИ

Китай стремится стать мировым лидером в области ИИ в рамках правительственной инициативы «Сделано в Китае 2025». Пекин считает, что технология ИИ является ключом к будущей глобальной военной и экономической конкуренции. В июле 2017 года Министерство промышленности и информационных технологий опубликовало «План развития искусственного интеллекта следующего поколения», в котором поставлены четкие цели: достичь того же уровня в области ИИ, что и США, к 2020 году, чтобы стать ведущим в мире центром инноваций в области ИИ к 2030 году и построить отечественную индустрию ИИ стоимостью 150 млрд юаней ($ 22,2 млрд) к 2020 году и 400 млрд юаней ($ 59,1 млрд) к 2025 году.

Китайский институт стандартизации электроники при Министерстве промышленности и информационных технологий является одним из ключевых игроков в стране. В 2018 году он выпустил «Белую книгу по стандартизации ИИ», в которой излагаются национальные рамки стандартизации ИИ и план по ее развитию. Китайские продукты в области

ИИ становится все труднее экспортировать по мере того, как на Западе растет внимание к стандартам конфиденциальности данных и угрозам безопасности (как видно из недавних опасений по поводу Huawei и 5G). Однако в целом китайская стратегия развития ИИ была признана самой всеобъемлющей и амбициозной в мире.

Страна также стремится к развитию международного партнерства в области ИИ в рамках своих усилий по установлению норм в этой области и экспорту своей практики государственного надзора в другие страны. В рамках своего цифрового Шелкового пути Пекин вкладывает значительные средства в цифровую инфраструктуру и в другие страны, чтобы распространить свой подход к ИИ, который, как надеется Пекин, приблизит эти страны к его собственной модели управления и сделает их более зависимыми от Китая. Связанное с этим тревожное событие – это тестирование и использование в Китае И И для цензуры, репрессий и широкомасштабного наблюдения в рамках таких инициатив, как его система социального кредита. Вдобавок к этому Пекин уделяет значительное внимание роли ИИ в обеспечении национальной безопасности, полагая, что интеграция ИИ в военные технологии может позволить Китаю обогнать Соединенные Штаты в военной отрасли.

Политика Китая в области ИИ также включает некоторые элементы международного сотрудничества в этой области. Основные из них – расширение сотрудничества с ведущи-

ми университетами в области ИИ и совместными исследовательскими центрами по всему миру; усиление своей роли в определении технологических стандартов; более активное участие в управлении ИИ, включая решение общих проблем (отчуждение роботов, контроль безопасности) и т. п.

Подход Европейского Союза к ИИ

Европейская Комиссия приступила к разработке своей стратегии ИИ в 2017 году, поручив Группе экспертов по ИИ разработать руководящие принципы для надежного и этичного использования ИИ в ЕС.

Вслед за этим в начале 2019 году Президент Еврокомиссии Урсула фон дер Ляйен объявила, что разработка всеобъемлющего законодательства в области ИИ будет приоритетом для ее Комиссии. Это привело к публикации Белой книги Комиссии по ИИ в феврале 2020 года. Предложения в Белой книге включают меры по оптимизации исследований и развитию сотрудничества в области ИИ между государствами-членами, а также увеличение инвестиций в разработку и внедрение ИИ на 70 %.

В последние годы европейские лидеры осознали важность того, чтобы не отставать в области ИИ и раскрыть свой потенциал. Такие лидеры, как канцлер Германии Ангела Меркель и Президент Франции Эммануэль Макрон, подчеркивали необходимость того, чтобы Европа стала ведущим гло-

бальным игроком в области ИИ, и новая Европейская Комиссия сделала ИИ приоритетом на следующие годы. Объявив ИИ основным стратегическим приоритетом, несколько государств-членов и институтов ЕС предпринимают шаги для продвижения амбиций Европы к лидерству в области ИИ. Это включает в себя разработку специальных документов по стратегии ИИ на национальном уровне и уровне ЕС, активизацию исследований и инноваций, а также изучение новых нормативных подходов к управлению разработкой и использованием ИИ.

Центральное место в усилиях ЕС занимает идея ИИ «создано в Европе», которая соответствует основным ценностям прав человека и демократическим принципам. На фоне опасений, что Европа уступает свои позиции Соединенным Штатам и Китаю, государства-члены ЕС понимают, что объем ресурсов, необходимых для того, чтобы идти в ногу с последними разработками в области ИИ, невозможно изыскать, действуя в одиночку. Существует четкое обоснование более сильной роли на уровне ЕС и более последовательного общеевропейского подхода к ИИ, который дополняет собственные действия государств-членов.

Ряд европейских стран, в частности Чехия, Эстония, Финляндия, Франция, Германия, Швеция и Великобритания, разработали собственные стратегии развития ИИ или планируют сделать это в ближайшем будущем. В той или иной степени эти стратегии предусматривают конкретные действия,

выделяют значительные суммы денег на развитие ИИ и стремятся отстаивать европейские ценности и продвигать ИИ этичным образом.

Подход Франции к ИИ был впервые изложен в правительственном отчете 2018 году (отчет Villani) под названием «За значимый ИИ: к французской и европейской стратегии». Этот стратегический документ воплощает всеобъемлющий и перспективный подход к ИИ, в котором особое внимание уделяется государственным исследованиям, ресурсам, обучению, трансферам и инновациям в таких стратегических секторах, как здравоохранение, окружающая среда, транспорт, а также оборона и безопасность.

В стратегии признается необходимость рассмотрения европейской экосистемы данных как общего блага, в котором государственные органы должны внедрять «новые способы производства, обмена и управления данными». В ней подчеркивается необходимость предотвратить утечку мозгов ведущих французских экспертов в этой области, сделать ИИ понятным для общества в целом, активнее проводить исследования и разработки в области технологий ИИ осмысленным и этичным образом. Э. Макрон объявил о выделении 1,5 млрд евро для государственного финансирования ИИ к 2022 году.

Стратегия Франции в области ИИ направлена на решение четырех основных задач: привлечение лучших специалистов, разработка политики открытых данных, особен-

но в тех секторах, где страна уже является конкурентоспособной, создание нормативно-правовой и финансовой базы, благоприятствующей развитию предприятий в области ИИ, и разработка нормативных актов в области ИИ с уважением к этике и приемлемым стандартам для граждан. С одной стороны, централизованный характер политической системы Франции может позволить правительственным агентствам устанавливать параметры для использования ИИ в определенных областях. С другой стороны, централизованное управление инновациями может в долгосрочной перспективе препятствовать прогрессу, поскольку ИИ требует широкого спектра НИОКР в различных областях. Кроме того, хотя Франция хорошо известна своими достижениями в области науки, технологий, инженерии и математики, по сравнению с Великобританией и Германией, во Франции отсутствуют академические учреждения и исследователи, активно и напрямую участвующие в исследованиях ИИ.

Согласно отчету «The Road to AI: Investment Dynamicsinthe European Ecosystem: AI Global Index 2019», к концу 2019 года Франция привлекла $ 1,2 млрд инвестиций для стартапов в области ИИ, что сделало ее лидером в Европе по финансированию ИИ, опередив Великобританию. Французская стратегия максимально учитывает этические соображения, связанные с ИИ (например, последствия использования беспилотных автомобилей, распознавания лиц и изображений, конфиденциальность). Французская страте-

гия детализирована и намечает конкретные шаги по повышению привлекательности страны для исследователей; повышению прозрачности и улучшению сотрудничества в области ИИ между различными участниками и т. п. Это одна из самых амбициозных европейских стратегий по развитию ИИ.

Французская стратегия ИИ выделяется своим нисходящим подходом под руководством правительства. Это показывает, насколько правительство считает ИИ стратегически важным. Дополнительным стимулом для развития ИИ является позиционирование Франции как лидера среди технологических стран после Брексита. Такие компании, как Google, Facebook, Uber, IBM, Samsung и Microsoft уже открыли или объявили о создании исследовательских центров ИИ в Париже.

Стратегия Великобритании в области ИИ в 2018 году претерпела несколько важных изменений. Было начато создание новых институциональных структур, таких как Управление по ИИ и Центр этики данных и инноваций. Был выпущен новый программный документ «Сделка в секторе ИИ», который будет способствовать сотрудничеству между различными правительственными агентствами и учреждениями, частными компаниями и академическими центрами. В апреле 2018 года правительство объявило об инвестировании почти 1 млрд фунтов стерлингов в «Сделку в секторе ИИ», в том числе 603 млн евро в виде новых государственных, про-

мышленных и академических инвестиций, и около 342 млн фунтов стерлингов добавится к ранее объявленному государственному финансированию.

В документе «Сделка в секторе ИИ» рассматриваются пять основ промышленной стратегии Великобритании: идеи, люди, инфраструктура, бизнес-среда и места. В нем также изложены пути реагирования на вызовы и возможности, предоставляемые ИИ, на основе: превращения страны в глобальный центр ИИ путем инвестирования в НИОКР, навыки и нормативные инновации; поддержки секторов для повышения производительности за счет ИИ и анализа данных; мирового лидерства в области безопасного и этичного использования данных и укрепления цифровых возможностей путем создания Центра этики данных и инноваций; а также помощи людям в развитии навыков, необходимых для работы в будущем.

Эти правительственные инициативы направлены на объединение существующих рассредоточенных и нескоординированных институциональных инициатив в различных технологических областях, таких как ИИ, автономные системы и робототехника, с тем чтобы удовлетворить амбиции Великобритании стать мировым лидером в этих областях. Хотя исследования ИИ в стране имеют глобальное влияние и, хотя в Лондоне самая высокая концентрация стартапов в области ИИ в Европе, а также сильная способность привлекать международные инвестиции в стартапы, коммерциализация

исследований традиционно является слабым местом для Великобритании.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, купив полную легальную версию на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.