УДК 34.096 **Юридические науки**

Шестопёрова Наталия Олеговна, *студент, 2 курс, направление подготовки «Правоохранительная деятельность 40.05.02» Саратовская государственная юридическая академия, г. Саратов*

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТА ВЕЩЕЙ

Аннотация: В данной научной статье проводится теоретико-правовой анализ понятия «интернет вещей», а также рассматриваются актуальные проблемы преступлений, связанных с использованием Интернета вещей. В дополнение проводится сравнительный анализ данного понятия и ее восприятии в России и зарубежных странах. Данная статья будет, несомненно, полезна, как специалистам в области информационных технологий и юридической сфере, так и самим гражданам, которые столкнулись с использованием IoT- устройств, предназначенных для повседневного пользования.

Ключевые слова: интернет вещей, преступление, устройства, конфиденциальность, защита данных, стратегия.

Annotation: This scientific article provides a theoretical and legal analysis of the concept of "Internet of things", as well as discusses current problems of crimes related to the use of the Internet of things. In addition, a comparative analysis of this concept and its perception in Russia and foreign countries is carried out. This article will undoubtedly be useful for both specialists in the field of information technology and the legal field, as well as for citizens themselves who are faced with the use of IoT devices intended for everyday use.

Keywords: Internet of things, crime devices, privacy, data protection, strategy.

Развитие информационно-коммуникационных технологий влияет на многие сферы жизни: политику, экономику, медицину, юриспруденцию и т.д. [1]. И Интернет вещей здесь не исключение, поскольку такие технологии окружают людей повсюду: и в рамках личных вещей, и внутри жилища, и в рамках «умного» города. Интернет вещей (далее - Internet of Things, сокращенно IoT) – это концепция, по которой устройства объединяются в одну сеть и взаимодействуют друг с другом [2]. Это помогает сделать устройства умными: они самостоятельно собирают информацию, обмениваются ей и принимают решения. Следить за состоянием и управлять ими можно с компьютера или телефона. Интернет вещей применяется в производстве, сельском хозяйстве, медицине, городской среде и в быту.

Актуальность данной темы состоит в том, что сейчас почти всё население нашей планы пользуется электронными устройствами и покупкой новых стараются все больше облегчить свою жизнь. Благодаря IoT (от англ. Internet of Things- сокр.IoT) устройства можно объединять в одну сеть, где они могут взаимодействовать друг с другом. В связи с возрастанием роли информации в наше время на первый план выходит её защита. Развитие интернета вещей может привести к различным проблемам, связанными с правовым регулированием передачи и использования личных данных пользователей. Так, уже ведутся активные дискуссии в обществе на предмет возможного нарушения конфиденциальности, кражи личных данных, доступа к информации и проблемам контроля. В данной работе я постараюсь выделить основные зоны риска в использовании IoT, которые могут стать причиной преступных посягательств злоумышленников.

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.

Соответственно любое нарушение целостности этих систем может быть предельно опасно для общества.

Идея, что устройства могут обмениваться информацией друг с другом без участия человека появилась достаточно давно. Еще в конце 70-х обсуждалась возможность полной автоматизации передачи данных. Тогда подобный подход назывался “повсеместные вычисления” (pervasive computing). Технологиям потребовалось несколько десятилетий развития для того, чтобы наконец стало возможным заговорить об Интернете вещей [3].

Во второй половине девяностых британец Кевин Эштон работал на компанию Procter and Gamble и занимался оптимизацией производства. Он заметил, что оптимизация напрямую зависит от скорости передачи и обработки данных. Когда сбором и обработкой данных занимаются люди, то на это могут уйти дни. Использование радиочастотной идентификации (RFID) позволило ускорить процесс передачи данных непосредственно между устройствами. Именно тогда и возникли вопросы по поводу обработки, сбора и распространения информации и данных без участия человека.

Потребовалось почти десятилетие для того, чтобы словосочетание «Интернет вещей» вошло в повседневную жизнь. Вместе с искусственным интеллектом IoT стал передовым направлением развития информационных технологий. Так, в 2008 году IPSO Alliance создал союз компаний, которые поддержали разработку технологий, связанных с Интернетом вещей. Это послужило сигналом для крупных корпораций.

Летом 2010 года стало известно, что сервис Google StreetView кроме показа панорамных фотографий умеет собирать данные об используемых Wi-Fi сетях. Эксперты заговорили о разработках нового протокола передачи данных, который позволит обмениваться данными между устройствами. В том же году Китай заявил, что планирует включить Интернет вещей в список приоритетных направлений исследований на ближайшие пять лет. Стало понятно, что сбором, обработкой и хранением данных заинтересовались не только крупные корпорации, но и правительства. В 2011 году занимающаяся исследованием

рынка компания Gartner включила IoT в свой лист наиболее перспективных развивающихся технологий.

Интернет вещей завоевывал мир. В 2012 году крупнейшая европейская интернет конференция LeWeb была посвящена данной теме, а такие журналы как Forbes, Fast Company и Wired начали активно использовать термин Internet of Things. Весь мир заговорил об Интернете вещей, а компании начали гонку технологий. В 2013 году IDC опубликовало исследование, в котором спрогнозировало рост рынка IoT к 2020 году до 8.9 триллионов долларов.

В январе 2014 года Google приобретает за 3.2 миллиона долларов компанию Nest, которая занималась разработкой устройств “умного дома” и созданием систем управления зданиями. Считается, что именно тогда рынок полностью признал — за Интернетом вещей ближайшее будущее. В том же году крупнейшая американская технологическая выставка Consumer Electronics Show прошла в Лас-Вегасе под вывеской Internet of Things. Так началась эпоха IoT.

Для развития интернета вещей правительства стран используют два вида инструментов: нормативно–регулятивный и аналитико–рекомендательный. От страны к стране соотношение этих инструментов может сильно различаться. Так, большинство стран заинтересовано в том, чтобы четко регламентировать вопросы безопасности, связанные с интернетом вещей. Технологические стандарты, как правило, не имеют обязательного характера. То же касается финансовых инструментов – они могут быть таргетированными, либо общего характера, либо вообще не применяться как мера стимулирования развития интернета вещей [4].

Принципы поддержки технологий интернета вещей в США находятся в русле общей государственной парадигмы развития научно–технологической и инновационной сферы. Роль государства заключается в создании экосистемы, способствующей появлению новых технологий. Основными элементами этой парадигмы являются стимулирование лидерства частного сектора в развитии технологий и стандартов, и разработка государственной политики при участии

всех заинтересованных сторон (стейкхолдеров). Для технологий интернета вещей государственная стратегия не разрабатывалась, однако отдельные ведомства обозначили важность данного направления. В 2008 г. Национальный разведывательный совет США назвал технологии интернета вещей прорывными.

Основной вопрос, который решают государственные ведомства США, состоит в определении таких стимулов к развитию интернета вещей, которые бы не стали преждевременными и чрезмерно ограничительными, но при этом обеспечивали бы безопасность для потребителей, в том числе и самих госструктур. Прямые меры поддержки, которые реализует американское правительство, сосредоточены преимущественно на создании «умных городов». В рамках инициативы Белого дома по Умным городам, в 2015 г.

«Умное» уличное освещение является одним из наиболее популярных способов применения Интернета вещей (IoT) в создании «умного города». В Сан-Диего пошли дальше, создав на основе системы уличного освещения сеть подключенных IoT-устройств, содержащих датчики света, звука и погоды, и передающих данные в открытую «облачную» платформу. Данные датчиков доступны сторонним разработчикам, которые находят неожиданные сценарии применения: например, датчики звука и алгоритмы триангуляции позволяют мгновенно определять место нарушения общественного порядка и передавать данные в полицию. Другие приложения позволяют информировать о наличии парковочных мест и локальных изменениях погоды. Затраты на создание системы составили порядка 30 млн. долларов. При этом только оптимизация управления освещением, и замена 35 тысяч источников света на современные светодиодные лампы позволит снизить энергопотребление на 60% и экономить около 2.5 млн. долларов в год.

В Атланте в 2017 г. внедрена система управления уличным движением, использующая данные из множества источников и элементы искусственного интеллекта. Источниками данных являются не только привычные предметы городской инфраструктуры, такие как светофоры и камеры, но и смартфоны

водителей, пешеходов и велосипедистов. Среди возможностей системы: автоматическое предоставление «зеленого коридора» автомобилям служб экстренного реагирования; автоматическое управление автомобильными и пешеходными светофорами; предупреждение о приближении опасно движущегося автомобиля для велосипедистов и пешеходов; предупреждение водителей о риске проезда на запрещающий [5].

В настоящее время Южная Корея ассоциируется с высокими технологиями, качественной медициной, высоким индексом развития человеческого потенциала и одной из сильнейших экономик. А Северная Корея, прочно связана с идеологией Чучхе, репрессиями, низким качеством жизни, недоеданием населения и культом личности. Но всё же высокие технологии начали развиваться и там.

В 2016 году в стране был запущен второй в мире (после Нидерландов) общенациональный интернет вещей. Сеть построена на базе технологии LoRaWAN (Long Range Wide-Area Network), обеспечивающей значительную экономию энергии. В первую очередь сеть объединит оборудование в коммунальных организациях и в домах их клиентов. В результате можно будет удалённо снимать показания счётчиков, подключать и отключать услуги.

Южная Корея славится не только своими передовыми технологиями, но и довольно жесткими законами. В 2016 году Парламент принял поправки к закону о содействии игровой индустрии: за производство и распространение читерских программ можно будет сесть в тюрьму на 5 лет или выплатить штраф в $43 тыс. А поскольку в Южной Корее создаётся основная масса читерских программ в мире, то новый закон сможет существенно облегчить жизнь всем честным игрокам.

В Сеуле для повышения эффективности вывоза мусора в пилотном режиме запущена программа Clean – мусорные баки с датчиками отслеживания наполнения подключены к облачной платформе Clean City Networks. В результате автоматического формирования маршрутов спецтехники на основании данных о наполненности баков удалось полностью исключить

случаи переполнения баков. Исключив поездки спецтехники к пустым бакам, удалось сократить пробег спецтехники на 66%, затраты – на 83%. Кроме того, жители стали активнее соблюдать правила сортировки мусора, увеличив долю отходов, направляемых на переработку, на 46%.

Развитие сегмента IoT (Internet of Things — интернет вещей) невозможно рассматривать вне глобальных трендов цифровой трансформации (частью которых и является сам Интернет вещей).

В развитых странах мира доля цифровой экономики уже составляет около трети от производимого в 2017 году ВВП [6].

Отставание России на фоне лидеров выглядит существенным вплоть до критичного: в 5 с лишним раз – от стран ЕС, в 7 раз – от США.

Эксперты отмечают российский феномен цифровизации: колоссальный разрыв между компаниями по уровню внедрения IT-технологий.

«С одной стороны – организации, которые находятся буквально на острие цифровой трансформации. С другой – целый пласт предприятий и организаций, не достигших даже базового уровня автоматизации процессов. Но избежать этого (промежуточного) этапа автоматизации – невозможно. Компании, которые его не пройдут, просто не попадут в цифровое будущее и быстро прекратят существование», — предупреждает генеральный директор IBS Светлана Баланова [7].

В силу специфики российской модели экономики, где госсектор играет доминирующую роль, эксперты IoT-отрасли уделяют большое значение роли государства в цифровой трансформации.

«Российское правительство ведет за собой частный сектор. А это очень отличается от того, что мы видим в других странах, где бизнес ведет за собой государство», — указывает главный экономист The World Bank Ханс Тиммер [8].

Что касается ключевых недостатков – они отчасти выражаются в неравномерном развитии нормативно-правовой и регуляторной базы: многие действующие нормативы, регламентирующие деятельность предприятий,

разработаны более 30 лет назад, еще во времена СССР.

Еще один системный минус в том, что Россия отстает от многих стран во внедрении именно тех IT-технологий, которые относятся к самым востребованным в мире: интернет вещей, робототехника, искусственный интеллект.

В Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы интернет вещей определен как «концепция вычислительной сети, соединяющей вещи (физические предметы), оснащенные встроенными информационными технологиями для взаимодействия друг с другом или с внешней средой без участия человека.» Это концептуальное определение, учитывающее компоненты «сети» и «датчики» и подчеркивающее такую характеристику интернета вещей, как автономность.

Концепция Интернета вещей не только приведет к модернизации отдельных инструментов и методов управления, но будет способствовать кардинальной перестройке функций управления, способов организации деятельности в современных компаниях [9]. Так, опыт глобальных компаний, уже внедряющих технологии IoT, показывает, что они способствуют повышению эффективности производства, значительному сокращению издержек на логистические, маркетинговые, административные процессы, позволяя уже сейчас строить предприятия нового типа (4.0 Industry). Но реализация этих технологических решений требует принципиально новых решений в области организации взаимодействия человека и машин, новых квалификационных характеристик от работников и новых методов не только управления производством, но прежде всего социального управления. Например, компания Airbus использует технологические решения, позволяющие объединить оборудование, промышленных роботов и машины в единую сеть Интернета вещей, предприятиям компании работать в максимально автономном режиме, существенно повысить качество сборки самолетов, отслеживая все операции в режиме реального времени. Однако внедрение подобных решений было связано со значительными затратами на

организацию взаимодействия объединенных в сеть машин с работниками с помощью средств и инструментов дополненной и виртуальной реальности.

Развитие концепции Интернета вещей будет приводить к трансформациям на рынке труда (причем не только региональном, но и глобальном), поскольку связано с потребностью в работниках нового типа, с другими профессиональными, процессуальными, организационными и даже социальными навыками и умениями. Внедрение IoT в деятельность организаций будет сопряжено с деквалификацией существующих сотрудников и необходимостью либо их переобучения, либо роста затрат на рекрутирование сотрудников с соответствующими знаниями и умениями из внешней среды. Ведущиеся в настоящий момент дискуссии по влиянию IoT на занятость сильно поляризированы: между сторонниками технологий, видящих в них безграничные возможности для формирования новых профессиональных групп, роста производительности текущих сотрудников, снижения процессов рутинизации труда, и их противниками, которые указывают на массовое замещение труда, значительное сокращение и даже исчезновение отдельных профессиональных групп, рост социального неравенства [10].

Развитие интернета вещей (от англ. Internet of Things- сокр.IoT) может привести так же и к различным проблемам, связанным с правовым регулированием передачи и использования личных данных пользователей. Так, уже ведутся активные дискуссии в обществе на предмет возможного нарушения конфиденциальности, злоупотребления данными, кражи личных данных, доступа к информации и проблемам контроля.

Пользовательские данные должны быть защищены от несанкционированного доступа, и эта безопасность должна обеспечиваться на каждом уровне связи. Таким образом, разнообразие устройств IoT и растущее число характерных каналов делают эту защиту сложной. Потенциальное влияние нарушений безопасности также возрастает, так как хранимые данные имеют все больше приложений, и, таким образом, предоставляют все больше и больше информации о пользователе и предоставляют все больший доступ к

особо важным сторонам нашей жизни.

Даже когда безопасность пользовательских данных может быть гарантированно защищена от несанкционированного доступа, вопрос о фактическом управлении и хранении информации поставщиком услуг остается открытым.

Вопрос о праве собственности на собранные данные также важен в связи с вопросом этики IoT: получение прав собственности или доступа к пользовательским данным, и перепродажа этих данных могут быть источником дохода.

Хотя сервис все больше и больше используется пользователем, этические вопросы (что происходит с пользовательскими данными, если пользователь покидает сервис, и насколько реально для клиента сменить поставщика услуг, предоставившего услугу долгое время) остаются без ответа. Эти вопросы важны для того, чтобы избежать перехвата данных потребителей, которые могут привести к несправедливому преимуществу, нарушению конкуренции, подавлению выбора потребителя, ухудшению качества обслуживания пользователей и снижению инноваций.

В связи с глобальным характером IoT и числом заинтересованных сторон, обязательно участвующих в развертывании IoT, возникает вопрос об ответственности и применимом законодательстве. Это подтверждается тем фактом, что различные субъекты IoT будут распространяться по разным странам и регионам, увеличивая число потенциальных законодательных актов. Этот вопрос важен не только для пользователей, которые могут быть сбиты с толку, какому законодательству они следуют, но и для политиков и всей цепочки создания стоимости и использования IoT, поскольку разработка приложений и развертывание IoT без четко определенной цепочки обязанностей и применимого права представляют собой сильные бизнес-риски.

Механизмы безопасности должны предотвращать «прослеживаемость» пользователей по всей сети, что, в свою очередь, может нанести ущерб конфиденциальности конечных пользователей, предоставляя злоумышленнику

данные, которые могут быть проанализированы с целью определения моделей поведения пользователя. Все эти проблемы приводят к так называемому “парадоксу конфиденциальности”: собирая личные данные, пользователям могут быть предложены лучшие «персонализированные» услуги; но эти личные данные могут быть обработаны методами интеллектуального анализа данных и собраны в профили пользователей, которые могут быть достаточно подробными, чтобы позволить идентифицировать пользователя. Когда эти «персональные данные» будут раскрыты, владелец данных не сможет контролировать, как сборщик данных будет их использовать.

Компьютерная безопасность включает в себя все процессы и механизмы, защищающие компьютерное оборудование, информацию и услуги от случайного или несанкционированного доступа, модификации или уничтожения. Следующие вопросы безопасности, связанные с IoT:

архитектура безопасности, которая описывает системные элементы, ответственные за управление безопасностью в течение жизненного цикла вещи;

модель безопасности узла, которая описывает, как параметры безопасности, процессы и приложения управляются в вещи;

загрузочная загрузка безопасности, которая определяет, как вещь может безопасно присоединиться к IoT в данном месте и в данный момент времени;

сетевая безопасность, которая описывает механизмы, применяемые в сети для обеспечения надежной работы IoT;

безопасность приложений, которая гарантирует, что только доверенные объекты могут взаимодействовать друг с другом.

Безопасность компьютерной сети состоит из мер предосторожности, принятых для предотвращения несанкционированного доступа, неправильного использования, модификации, блокировки компьютера и сетевых ресурсов, доступных через сеть. Сетевая безопасность включает авторизацию данных доступа к сети, которой управляет сетевой администратор. Интернет является небезопасным каналом обмена информацией, что приводит к высокому риску мошенничества или перехвата личных данных пользователя. IoT основан на

компьютерных сетях и Интернете для поддержания связи между объектами, а также между людьми и вещами, поэтому он имеет отношение ко всем вопросам компьютерной сети и безопасности Интернета. Перед использованием смарт-чипов, компании и государственные органы должны оценивать их влияние на конфиденциальность и защиту данных. На основе этих оценок, сертифицированных национальными органами по защите данных, должна быть обеспечена безопасность персональных данных и надежная безопасность

Как и традиционная преступность, киберпреступность имеет много различных аспектов и может происходить в самых разных сценариях. Существующие определения киберпреступности различаются в зависимости от точки зрения жертвы, защитника и наблюдателя. Ньюмен определяет киберпреступность как поведение, в котором компьютеры или компьютерные сети являются инструментом, целью или местом преступной деятельности. Это включает как средства и методы совершения нападений на информационные активы, так и использование компьютеров для совершения “традиционного” преступления. В Договоре о киберпреступности Совета Европы термин “киберпреступность” используется для описания различных преступлений, начиная от преступной деятельности против данных и заканчивая нарушением авторских прав. "Руководство Организации Объединенных Наций по предупреждению преступности, связанной с использованием компьютеров, и борьбе с ней" также включает несанкционированный доступ, мошенничество и подделку в свое определение киберпреступности.

Конвенция Совета Европы о киберпреступности постулирует четыре различных вида преступлений:

1) преступления против целостности, конфиденциальности и доступности компьютерных данных и компьютерных систем;

2) преступления, связанные с компьютерами;

3) преступления, связанные с содержанием программного обеспечения;

4) преступления, связанные с авторским правом.

Сетевые преступления включают в себя вмешательство в функции

компьютерной сети путем ввода, передачи, повреждения, изменения или подавления сетевых данных. Преступления, связанные с доступом, относятся к несанкционированному доступу и распространению вирусов. Преступления, связанные с контентом-– нарушения авторских прав, незапрошенные коммерческие сообщения и кибер-угрозы.

Киберпреступность эволюционировала от традиционных преступлений (таких как мошенничество) в результате технического прогресса, который расширил пространство обычных преступлений, предоставляя более (изощренные) средства, больше возможностей, новых оснований и целей действий. Что касается общих средств, то информационно- коммуникационные технологии (ИКТ) расширяются как для ускорения, так и для охвата преступной деятельности. Возможность часто рассматривается как еще один решающий элемент или даже как первичный провоцирующий фактор в инициировании преступного деяния. Интернет сам по себе является богатой возможностями средой для преступной деятельности, поскольку он изначально не был разработан с учетом безопасности. В дополнение к повышению доступности преступных объектов также расширяет возможности доступа к информации, инструментам и поддержке для совершения преступлений. Наконец, широкое измерение и сложность кибернетического контекста открывают возможности для сокрытия преступлений от общественности в силу виртуального характера преступных методов.

Интернет вещей (IoT) создает новые проблемы для защиты данных и конфиденциальности конечных пользователей: пользователи не захотят принимать IoT, который невидимо смешивается с их средой обитания, не будучи уверенными в том, что безопасность частной информации гарантируется и обеспечивается адекватная безопасность. Соединяя все "вещи" в глобальной инфраструктуре интернета и имея "вещи", сообщающиеся друг с другом, возникают новые проблемы безопасности и конфиденциальности, например, конфиденциальность, подлинность и целостность данных, воспринимаемых и обмениваемых "вещами". В целом же, безопасность людей

и вещей в IoT должна быть обеспечена должным образом для предотвращения и борьбы с киберпреступлениями.

Таким образом, Интернет вещей является передовой технологией, способной облегчить деятельность врачей, логистов, организаторов и т.д. Вместе с тем, нельзя забывать о необходимость защиты прав и свобод человека и гражданина, общества, государства [11]. Надлежащее регулирование составов киберпреступлений, выработка правовой позиции Верховным Судом РФ, будет способствовать эффективному применению Интернета вещей на благо всего общества.

Библиографический список:

1. Лескина Э.И. Применение блокчейн-технологий в сфере труда // Юрист. 2018. № 11. С. 25.
2. Что такое Интернет вещей и как он поможет предприятиям зарабатывать больше? URL: https://habr.com/ru/post/474796/ (дата обращения: 27.09.20).
3. История Интернета вещей. С чего все начиналось? URL: https://perenio.ru/blog/the-history-of-the-internet-of-things (дата обращения: 27.09.20).
4. Дежина И. Г. Перспективные рынки и технологии Интернета вещей. Москва, 2019. С. 91. (дата обращения: 29.09.20).
5. Применение технологий Интернета вещей для развития современной городской среды URL: www.pwc.ru/IoT (дата обращения: 30.09.20)
6. Доклад партнера Bain & Company Лорана-Пьера Бакулара на форуме «Открытые инновации», 2018 (дата обращения: 02.10.20).
7. Выступление генерального директора IBS Светланы Балановой на форуме «Открытые инновации», 2018 (дата обращения: 02.10.20).
8. Выступление главного экономиста The World Bank Ханса Тиммера на форуме «Открытые инновации», 2018 (дата обращения: 02.10.20).
9. Маркеева А. В. Интернет вещей (IOT): возможности и угрозы для

современных организаций URL: file:///C:/Users/User/Downloads/internet-veschey-iot-vozmozhnosti-i-ugrozy-dlya-sovremennyh-organizatsiy%20(1).pdf (дата обращения: 02.10.20).

10. Маркеева, А. В. Интернет вещей (IOT): возможности и угрозы для современных организаций/ А. В. Маркеева// Научная статья. – 2016. – С. 3 (дата обращения: 02.10.20).

11. Мишутина Э.И. Аксиологические аспекты в гражданском процессуальном праве: автореферат дисс. на соискание ученой степени кандидата юридических наук. Саратов, 2012.