



УДК 004.738.5

ИЗУЧЕНИЕ РИСКОВ ИНТЕРНЕТА ВЕЩЕЙ**Стрельников Евгений Владимирович**

студент

Поволжский государственный технологический университет, г. Йошкар-Ола

Аннотация. Интернета вещей – это способность собирать данные с помощью датчиков и передавать их через Интернет, однако нельзя утверждать, что сбоев при создании такой системы не будет, поэтому необходимо иметь представление, какие последствия могут оказать те или иные сбои в работе системы интернета вещей.

Ключевые слова: Интернет вещей, интернет, компьютерные технологии устройства.

Интернет вещей – это не поразительное изобретение, вроде машины для очистки хлопка. Промышленность не будет поймана врасплох в мышеловку, которая сделает производственные системы и продукты устаревшими.

Мы не можем утверждать, что сбоев не будет поэтому необходимо иметь представление, какие последствия могут оказать те или иные сбои в работе системы интернета вещей.

Конфиденциальность. Сегодня в мире миллиарды датчиков постоянно получают данные о своем окружении, которое включает людей, то проблемы конфиденциальности имеют огромное значение. Большинство развитых стран мира предприняли попытки защитить потребителей от незаконного использования конфиденциальной информации. Но во многих случаях законы не являются универсальными для регулирования огромного количества новых способов, благодаря которым личная информация накапливается и используется. На ранней стадии развития Интернета потребители познакомились, с таким отслеживающим программным обеспечением, как cookie. Так как не было никаких конкретных законов, ограничивающих использование их веб-сайтом с целью отслеживания поведения пользователя при просмотре страницы, многие компании просто использовали их, не беспокоясь о мнении пользователей. И только поисковые компании ответили на беспокойство граждан и их потребность в инструментах, которые ограничивают использование cookie и удаляют их после посещения того или иного сайта. Вопросы конфиденциальности распространяются и на рабочее место. Существует много программ, которые позволяют работодателю отслеживать поведение сотрудника, как правило, с помощью его компьютера. Благодаря Интернету вещей встроить датчики можно практически в каждый угол офиса, чтобы контролировать действия персонала. Некоторые компании так и делают, что вызывает возмущение пользователей.

Кибербезопасность. Кибернарушения являются серьезной угрозой для бизнеса сегодня.



Согласно некоторым оценкам, ежегодно киберпреступность обходится предприятиям в 400 млрд долларов США. Наиболее тревожно с точки зрения Интернета вещей то, что киберпреступники легко взламывают якобы безопасные системы с несколькими уровнями защиты. Сложность с обеспечением безопасности устройств Интернета вещей – это область, требующая улучшений. Вопросы безопасности устройств на технологиях Интернета вещей особенно актуальны в рамках подготовки к появлению экосистемы Интернета вещей, когда миллиарды объектов будут подключены к Интернету и соединены между собой. Любое устройство с доступом в Интернет является потенциальной точкой входа для хакера. Город, который строит умную систему электроэнергетики, может ощутить масштабы возможной экономии от того, как система упрощает поиск и устранение неисправностей. В то же время сама система дает потенциальному хакеру возможность легко остановить электропитание всего города при помощи компьютера. Иными словами, хакер-террорист может использовать систему в своих личных целях. Также, из-за сетевого характера Интернета вещей, когда каждый подключенный объект использует данные других подключенных объектов, есть также риск того, что неисправность может привести к катастрофическому сбою системы. Неисправный объект может передать неправильные данные другому устройству, которое функционирует нормально. А когда некорректные данные распространяются по системе, они начинают заражать все больше и больше систем. Данные примеры подчеркивают новые риски, с которыми столкнутся многие предприятия, когда дело дойдет до кибербезопасности Интернета вещей. В то же время мы можем ожидать, что производители этих устройств будут своевременно повышать меры безопасности, так как огромное количество подключенных объектов растет в геометрической прогрессии.

Ответственность. Когда дело доходит до автономных транспортных средств, таких как автомобили без водителя, мы сталкиваемся с очевидной этической дилеммой: за секунды до аварии должно ли автономное транспортное средство сделать все, что может, чтобы защитить пассажиров, даже если это означает нанесение вреда другим автомобилистам или пешеходам? Когда за рулем находятся люди, сопутствующий ущерб, каким бы страшным он ни был, не представляет большой этической проблемы. Водитель, действующий инстинктивно в чрезвычайной ситуации, может быть признан виновным, если его инстинкт самосохранения заставит его совершить наезд на пешехода, например. Но когда решение принимает машина, может ли пешеход, пострадавший в аварии, подать иск против производителя автомобилей? Может ли водитель подать иск против производителя автомобилей вследствие аварии, в которой он получил травмы? Другие вопросы ответственности возникают, при рассмотрении право собственности на данные. С миллиардами устройств, которые их собирают, становится не ясно, кто несет ответственность за какие данные., поскольку объекты Интернета вещей



функционируют автономно и в сочетании со многими другими объектами.

Таким образом, вопрос о надежности и рисках, а также регулирования спорных ситуаций, связанных с реализацией Интернета вещей остается открытым.

Список литературы:

1. Алексей Лагутенков. Тихая экспансия интернета вещей // Наука и жизнь. – 2018. – № 5. – С. 38–42.
2. Интернет вещей: эволюция или революция? / Официальный сайт компании American International Group» [Электронный ресурс]. – URL: <https://www.aig.ru/>
3. Леонид Черняк. Платформа Интернета вещей [Электронный ресурс]. –URL: <https://www.osp.ru/os/2012/07/13017643>