

Новые технологии



Михаил Чукин, Владимир Зяблицев



Ульяна Михайлова



Егор Картавец, Максим Дунаев, Екатерина Горлова



Дружить – так с роботом?

Искусственный разум может быть опасен

«Умные дома» снимают и показывают владельцев. Зубная щётка передаёт данные о местонахождении, смарт-TV отсылает информацию о любимых сайтах и передачах. Телефон «рассказывает», когда человек просыпается, а машина или даже самолёт могут зажить собственной жизнью. Это и многое другое обсудили в МГТУ на встрече, посвящённой умным гаджетам.

Электронная торговля

Ректор вуза Михаил Чукин отметил важность темы. Ведь освоение смарт-устройств неуклонно продолжается. Ожидается, что большинство пользователей перейдёт на подключение к Интернету с мобильных устройств. Председатель правления общественной организации «Объединение защиты прав потребителей» Магнитогорска Владимир Зяблицев отметил, что новые технологии – это прекрасно, но зачастую они не только помогают нам, но и вызывают проблемы. Особенно если не уметь правильно пользоваться гаджетами.

– В России 73 процента населения «сидит» в Интернете, – рассказал Владимир Иванович. – В конце прошлого года правительство утвердило паспорт национальной программы «Цифровая экономика РФ». Её основные цели – безопасность и просвещение. За ближайшие шесть лет десять миллионов человек пройдут обучение по специальным программам.

Без подобных знаний в современном мире сложно. Например, интернет-магазины уже сейчас успешно вытесняют традиционные торговые форматы. Оборот онлайн-торговли за четыре года увеличился в три раза. Специалисты предполагают, что в недалёком будущем потребители окончательно перейдут на электронные торговые площадки – маркетплейсы.

Там производители товаров и исполнители услуг будут размещать свои предложения, а доставят приобретённые товары логистические компании, победившие в конкурентной борьбе.

– Вместе с тем становится больше случаев, когда заказанный товар не пришёл вовремя, оказался не тем или плохого качества, – отметил Владимир Иванович. – Бывает, что услуга после оплаты и вовсе не оказывается. Потребитель зачастую не может предъявить претензию своему контрагенту, потому что информация о нём неполна или недостоверна. И в этом случае ответственность должен нести агрегатор, что и предусмотрено поправками в закон «О защите прав потребителей», вступившими в силу с начала этого года.

Напомним, агрегатор – тот, кто собирает и группирует объекты. Это могут быть сервис-провайдеры, операторы связи, авиакомпании. Союзы защиты прав потребителей добиваются, чтобы агрегаторы не выкладывали информацию о товарах и услугах, если нет полных и внятных данных о продавце.

Умные шпионы

Доцент кафедры информатики и информационной безопасности МГТУ Ульяна Михайлова отметила, что в современном цифровом обществе уже невозможно представить жизнь без различных гаджетов и умных устройств. Смарт-девайсы созданы для расширения функционала обычных вещей и значительно превосходят их по возможностям. По сути, все эти устройства представляют собой компьютеры, подключённые к Интернету. Уже стали трендом и «умные дома», позволяющие со смартфона управлять оборудованием. Они максимально упрощают жизнь, рационально используют время, деньги и силы. Это вроде бы повышает безопасность и обеспечивает контроль, а также энергоэффективность.

– Есть и недостатки, – отметила

Ульяна Владимировна. – Для установки множества приложений и создания аккаунтов, возможно, понадобится помощь постороннего человека. Гаджеты разных производителей могут плохо работать, а то и вовсе не сосуществовать вместе. Так что придётся покупать товары одной компании.

Вдобавок устройства постоянно обновляются, и невозможно предсказать, какими функциями будет обладать тот или иной прибор в будущем. А самые большие минусы – это сомнительные безопасность и конфиденциальность.

– Если хакеры получают доступ к системе управления «умного дома», они смогут отключить свет, сигнализацию, открыть дверь и выполнить любые действия, – пояснила преподаватель вуза. – Прецеденты уже есть. Многие системы круглосуточно записывают видео и хранят их потом в приложении. Они фиксируют и отправляют по сети смарт-устройства время завода будильника, статистику включения и выключения света. ТВ-провайдеры передают компаниям, какие передачи и фильмы чаще всего смотрят хозяева, зубная щётка способна передавать данные о местоположении. По потоку данных можно вычислить, когда хозяева уехали в отпуск и куда. Видеокамеры и голосовые колонки связываются с серверами компании каждые две минуты, независимо от того, в каком режиме находятся.

Фальшивые отпечатки

Ульяна Михайлова сомневается и в надёжности биометрических данных, хотя система ещё только внедряется в России. В банковской сфере она начала появляться с июля 2018 года. Сервис позволяет стать клиентом финансовых учреждений и получать услуги без посещения офисов и предъявления паспорта – с помощью биометрии. Впоследствии подобная система может перейти и в другие сферы жизни. Между тем, как рассказала специалист по информационной безопасности, отпечаток пальца с помощью силиконовой наклейки подделывается за час, лицо с 3D-муляжом – в течение дня. Давно не проблема подражание или запись голоса. Можно точно скопировать даже радужку глаза.

– В ближайшем будущем эксперты предлагают заменить биометрическую аутентификацию на биочипирование, – отметила Ульяна Владимировна. – В перспективе чип может заменить паспорт,

налоговый код, социальную и пенсионную карты, избавит от необходимости иметь наличные деньги. Недостатки чипов – прямое продолжение их достоинств. Нет полной гарантии безопасности, безвредности и технической надёжности. И главное: когда чип станет документом, удостоверяющим личность, кошелем и ключом от всех дверей, то человек будет на сто процентов подконтрольным. В один миг его можно сделать нищим – заблокировать средства на счету, бездомным – электронный замок не откроется, а также безымянным – попробуй докажи, что это ты.

Ульяна Михайлова добавила, что чип вряд ли будет вшиваться в голову. По крайней мере, в ходе первых экспериментов чаще всего используются руки. Так что абсолютной «матрицы», как в кино, всё равно не будет. Больше беспокоиться нужно, наверное, о другом.

Сбой контроля

– Люди стали доверять умным устройствам не только личные данные, деньги и дома, но и собственные жизни, – тревожится преподаватель кафедры информатики. – Уже можно заказать беспилотные такси в Сколково. Запущено тестирование, чтобы ввести подобные технологии в систему обычного городского транспорта. Между тем специалисты отметили сходство крушений авиалайнеров в Индонезии и Эфиопии. Боинги были оснащены умными системами. Предполагается, что именно они выдали ошибочные показатели системы контроля полёта. Оказывается, искусственный разум способен вести самолёты в крутое пике, и пилоты ничего не могут с этим сделать. Пока неясно, почему они не выполнили штатную процедуру по отключению автоматической системы.

Ульяна Михайлова дополнила страшную картину информацией о почти двух тысячах компаний, которые каждую минуту становятся жертвами киберпреступников. Рассказала, что мировая экономика из-за этого теряет более одного миллиона долларов. Наиболее подвержены атакам сферы образования, финансов, госсектор, производство и транспорт. Между тем участники крупнейшего международного экономического форума в Давосе пришли к выводу, что искусственный интеллект и машинное обучение станут ключевыми технологиями четвёртой промышленной революции. Мир заполонят «умные машины», осна-

щённые не только Интернетом, но и способностями к самостоятельному принятию решения.

– Мы с вами не сможем избежать этой революции, но не надо воспринимать её как безоговорочное благо, – попросила преподаватель МГТУ. – Необходимо обезопасить себя от её рисков. Если не будем развиваться в данном направлении и понимать суть умных устройств, можем превратиться в чипированных питомцев роботов.

Берегите себя

Свой вклад в описание опасного образа новых технологий внесли и студенты из института энергетики и автоматизированных систем. Егор Картавец рассказал о социальных сетях. Это сервис, который позволяет строить отношения, общаться, заключать сделки, играть, участвовать в акциях. Популярность соцсетей оправдана, но есть и опасность. Максим Дунаев обратил внимание на то, что большая часть друзей в Сети – ненастоящие. Вдобавок на страницах выкладывается слишком много личной информации. Это может навредить. Для проверки учащихся и преподавателям предложили зайти на сайт поиска человека по изображению. Некоторые сделали селфи, кто-то сфотографировал соседа по парте. Результат неприятно удивил. Около картинки очень быстро появилась масса информации об изображённом человеке, а также о его друзьях, знакомых, родных и домашних питомцах.

Екатерина Горлова отметила плохую и медленную работу технической поддержки в социальных сетях и рассказала о мошенниках. Граждане регулярно встречают обманщиков, создающих фальшивые благотворительные фонды или ссылки на вредоносные сайты, выманивающие явки и пароли. Очень распространены предложения о подарках, выигрышах – заплатить надо только за пересылку или доставку. Не очень хорошо, как пояснили студенты, обстоят дела и со свободой слова. Причём пострадать можно не только за фразы, но и за лайки, репосты. А ещё нужно быть осторожнее с троллями, которые провоцируют пользователей на эмоции, преследуя коммерческие или политические цели.

– Мы не призываем вас становиться параноиками, – было сказано в заключение. – Но не стоит забывать об опасности. Будьте осторожны. Берегите себя и свои страницы.

Татьяна Бородина