УДК 004.716

ИНТЕРНЕТ ВЕЩЕЙ: ИННОВАЦИОННАЯ ОПАСНОСТЬ ФИНАНСОВОГО СЕКТОРА ЭКОНОМИКИ РФ

Воеводин А.Ю., Хатырева А.С.,
студенты, Финансовый университет
andr.voevodin@mail.ru
khanser1012@gmail.com

Аннотация. *В данной статье рассмотрено влияние концепции Интернета вещей на банковскую деятельность, выявлены основные преимущества и барьеры, препятствующие развитию IoT в сфере финансовых услуг. В результате проведенных исследований выявлены основополагающие методы и принципы защиты Интернета вещей.*

Ключевые слова: *Интернет вещей; финансовый сектор; банковская деятельность; сети связи; кибератака; безопасность.*

THE INTERNET OF THINGS: INNOVATIVE HAZARD OF THE FINANCIAL SECTOR OF THE ECONOMY OF THE RUSSIAN FEDERATION

Voevodin A.Y., Khatyreva A.S.,
students, Financial University
andr.voevodin@mail.ru
khanser1012@gmail.com

Abstract. *This article examines the impact of the concept of the Internet of things on banking activity, identifies the main advantages and barriers that impede the development of the IoT in financial services. As a result of the research, fundamental methods and principles of protecting the Internet of things were defined.*

Keywords: *The Internet of Things; financial sector; banking activity; яommunication networks; cyberattack; security.*

Несмотря на то что первое упоминание термина «Интернет вещей» (англ. Internet of Things, IoT) встречается с 1999 г., единая, общепринятая терминологическая база в рассматриваемой предметной области до сих пор окончательно не сформирована. В рамках данной статьи под Интернетом вещей будем понимать расширение возможностей подключения к сети и вычислительных способностей для объектов, устройств, датчиков и других предметов, обычно не считающихся компьютерами.

Ряд компаний и научно-исследовательских организаций делают многочисленные прогно-

Научный руководитель: ***Дворянкин С.В.,*** *доктор технических наук, профессор, заместитель заведующего кафедрой информационной безопасности.*

зы относительно потенциального воздействия IoT на мировую экономику в течение ближайших пяти или десяти лет. Например, согласно исследованиям McKinsey Global Institute, финансовое влияние IoT может достигнуть от 3,9 до 11,1 млрд долл. США к 2025 г. Очевидно, что для Российской Федерации важно находиться в числе лидеров по внедрению и развитию таких технологий.

Вопросы безопасности IoT

При постоянном увеличении числа устройств, подключенных к Интернету, неизбежно возникновение новых потенциально уязвимых мест. Если устройство недостаточно защищено, оно может служить точкой доступа для кибератаки, давая возможность злоумышленнику перепрограммировать данное устройство или сделать его неисправным [1].

Необходимо понимать, что безопасность устройств, подключенных к Интернету вещей, не является бинарным понятием защищенности или незащищенности. Безопасность IoT устройств — это диапазон уязвимости: от незащищенности до высшей степени безопасности с несколькими уровнями защиты.

Оценка рисков и возможных последствий включает в себя целый ряд факторов: наличие четкого понимания существующих рисков безопасности и потенциальных рисков в будущем; приблизительные экономические и другие последствия в случае осуществления рисков; приблизительную стоимость устранения их последствий.

С принципиальной точки зрения разработчики интеллектуальных предметов для Интернета вещей обязаны гарантировать, что эти устройства не будут подвергать опасности своего владельца или других людей.

С точки зрения бизнеса и экономики производители заинтересованы в уменьшении затрат, снижении уровня сложности и сокращении времени до выпуска изделия на рынок. Недостаточный уровень безопасности устройств IoT приводит к отрицательным внешним последствиям, где затраты возлагаются одной стороной (или сторонами) на другие. В случае информационной безопасности внешние проблемы возникают в тех случаях, когда производитель продукта не несет ответственности за затраты в результате недостаточного уровня безопасности.

Также необходимо заметить, что устройства IoT имеют ряд уникальных проблем безопасности. Например, многие из этих устройств смогут самостоятельно устанавливать связь друг с другом непредсказуемым и динамическим способом. В результате потенциальное число взаимных подключений между этими устройствами является беспрецедентным.

Многие системы IoT будут состоять из групп идентичных или почти идентичных устройств. Такая однородность усиливает потенциальное воздействие каждой уязвимости, умножая его на количество устройств, имеющих те же характеристики.

Развертывание многих устройств, подключенных к Интернету вещей, будет осуществляться с учетом срока эксплуатации, на много лет превышающего обычные сроки для высокотехнологичного оборудования. Развертывание этих устройств может осуществляться в условиях, затрудняющих или делающих невозможной их модернизацию или изменение конфигурации. Эти устройства могут пережить своего производителя и остаться без технической поддержки в долгосрочной перспективе. Такие сценарии демонстрируют то, что механизмы безопасности, работающие в момент развертывания, могут быть непригодны для всего срока службы устройств по мере появления новых угроз. В результате это может привести к появлению уязвимостей, которые будут сохраняться в течение длительного времени.

Многие устройства IoT изначально не предполагают возможности обновления либо эта процедура слишком неудобна и непрактична. В качестве примера можно привести отзыв 1,4 млн автомобилей Fiat Chrysler в 2015 г. [2] для устранения уязвимости, благодаря которой злоумышленник смог взломать автомобиль с помощью беспроводной сети.

Многие устройства IoT работают таким образом, что пользователь не имеет или почти не имеет представления о внутреннем функционировании устройства или создаваемых им потоках данных. Это создает уязвимость в области безопасности. Пользователь считает,

что устройство IoT работает по определенному направлению, в то время как на самом деле оно может выполнять нежелательные действия или собирать данные, которые пользователь не намерен предоставлять. Функции устройства также могут изменяться без предупреждения при обновлении, в результате чего пользователь подвергается опасности из-за любых изменений, вносимых производителем.

Некоторые устройства IoT устанавливаются в таких местах, где трудно или даже невозможно обеспечить их физическую безопасность. Злоумышленники могут получить к ним прямой физический доступ. В связи с этим для обеспечения безопасности необходимы функции защиты от взлома и другие инновации.

Некоторые устройства IoT, такие как датчики состояния окружающей среды, незаметно встраиваются в элементы окружения, где пользователь не замечает их и не может контролировать. Кроме того, устройства могут не иметь функции предупреждения о возникновении проблем безопасности, в результате чего пользователь может не знать о наличии угрозы.

IoT в банкинге

Преимущества IoT в банковском маркетинге и финансовых сервисах:

- Сбор данных постоянно и в режиме реального времени.

Например, страховщик может оценить реальные модели использования застрахованного автомобиля. Он также может установить правила, по которым можно дистанционно заблокировать модели поведения автомобиля (превышение скорости и т.д.).

- Действия клиента могут вызывать ответные маркетинговые действия.

Например, установленный в дверь магазина маяк может распознавать телефон или RFID и предлагать индивидуальный кэшбэк.

- Мгновенный обмен данными между устройствами.

Например, можно использовать в магазинах сканеры для идентификации продуктов в корзине и мобильного бумажника клиента, сам же покупатель будет использовать для оплаты RFID [3].

Основные барьеры для развития IoT в сфере финансовых услуг и банковского маркетинга:

- конфиденциальность и вопросы безопасности;
- соблюдение установленных норм;
- отсутствие общих стандартов.

В августе 2015 г. IDC (International Data Corporation — ведущий поставщик информации, консультационных услуг и организатор мероприятий на рынках информационных технологий, телекоммуникаций и потребительской техники) был проведен опрос. Согласно этому исследованию 58,4% тех, кто принимает решения в финансово-промышленной сфере, рассматривают IoT как «стратегические» инициативы; 20% полагают, что это лишь «трансформационные» инициативы и лишь 5,6% респондентов сказали, что влияние IoT не играет роли [4].

Нет никаких сомнений в том, что развитие IoT в банковской и финансовой сферах услуг будет поддерживаться следующими факторами:

1. Технический прогресс делает IoT более доступным и стандартизованным.
2. Массовое принятие технологий IoT.
3. Конкуренция в финансово-техническом секторе (мобильные платежи и т.д.).

Рост может быть замедлен несоответствием нормативным требованиям, особенно в конфиденциальности данных, но в целом неизбежен. Ниже приведены примеры использования IoT в банкинге, которые четко показывают конкурентное преимущество данной технологии.

Примеры IoT в сфере банковских и финансовых услуг

- *Visa Mobile Location Confirmation*

Компания Visa запускает сервис под названием “Mobile Location Confirmation”, который позволит отслеживать местонахождение держателя карты автоматически. Он будет сопоставлять эту информацию с информацией о месте расходования средств, помечая транзакцию как надежную, если они совпадают. Данная мера обещает стать эффективным инструментом в борьбе с мошенничеством. Новая услуга будет полностью добровольной. Пользователь в любой момент сможет от нее отказаться, используя мобильное приложение. Никакие данные, полученные от пользователя, не будут использоваться в маркетинговых целях, обещают в компании [5].

Мошенничество с использованием кредитных и дебетовых карт очень дорого обходится потребителям и банкам, в одном только 2012 г. ущерб составил 4 млрд долл. США. Учитывая это, банки и платежные системы постоянно пытаются улучшить безопасность использования банковских карт.

- *Sense by Alfa-Bank*

На конференции Finovate представители «Альфа-Банка» представили персонального финансового ассистента Sense. Это приложение может давать подсказки пользователю на основе его трат.

Sense использует машинное обучение и подсказывает, что может понадобиться клиенту. Приложение получает информацию о привычках пользователя исходя из его трат, а также данных от других сервисов, которые подключаются к Sense.

В частности, Sense может напомнить о долгах или оплате счетов, а также разделить траты с друзьями. Если пользователь пошел на вечеринку, то в какой-то момент сервис может понять, что мероприятие закончилось, и вызвать такси [6].

- *Groceries by MasterCard*

MasterCard и Samsung представили на выставке CES встроенное в смарт-холодильник решение, с которым покупка продуктов для всей семьи станет еще проще, быстрее и удобнее. Приложение Groceries by MasterCard позволяет выбирать и оплачивать продукты прямо на дисплее нового смарт-холодильника Samsung Family Hub.

Приложение Groceries связывает ведущие продуктовые магазины и покупателей самым удобным и эффективным путем — через кухню. Оно помогает переосмыслить привычный способ совершения покупок для всей семьи и предлагает ее членам создавать, редактировать и обмениваться шопинг-списками с любого мобильного устройства. Запомнив предпочтения членов семьи, приложение от MasterCard подбирает в онлайн-магазинах нужные товары. Если требуется добавить продукты в онлайн-корзину — достаточно выбрать понравившийся продукт либо на дисплее холодильника, либо на экране своего смартфона.

Также приложение позволяет контролировать семейные расходы: финальный список утверждается введением четырехзначного пин-кода [7].

Принципы защиты IoT

Первый важный шаг в обеспечении безопасности устройства заключается в том, чтобы гарантировать, что пользователь действительно является тем, за кого себя выдает, и действительно имеет право для доступа к этому устройству. Процедура аутентификации является важным аспектом при работе с подключенными устройствами. Например, когда мы открываем свой умный автомобиль с помощью мобильного телефона, мы должны быть уверены, что никто кроме нас не сможет этого сделать.

Для более надежной аутентификации все чаще используются биометрические данные, например отпечатки пальцев или сканирование сетчатки, которые позволяют достоверно подтвердить, что мы являемся именно теми, за кого себя выдаем.

Но на самом деле автомобили далеко не всегда обладают хорошей защитой, как можно подумать! Австралийский исследователь в области безопасности Сильвио Сезаре (Silvio Cesare) продемонстрировал уязвимость в устройстве электронного замка автомобиля, в результате которой он сумел отключить сигнализацию и проникнуть в автомобиль, не оставив после себя никаких улик для полиции. При этом для получения доступа к автомобилю он использовал простейшую программно-определяемую радиосистему (software defined radio) и антенну, с помощью которых он мог перехватывать и отправлять беспроводные сигналы.

Поставщики оборудования также должны быть авторизованы для доступа к удаленному устройству. Производитель электромобиля Tesla оповещает водителей о доступности обновления прошивки и о том, когда это обновление будет загружено. Таким образом, водитель понимает, что обновление было по-

лучено непосредственно от Tesla и что это не попытка злоумышленника проникнуть в систему. Для более надежной аутентификации все чаще используются биометрические данные, например отпечатки пальцев или сканирование сетчатки, которые позволяют достоверно подтвердить, что мы являемся именно теми, за кого себя выдаем.

Анализ ситуации показывает необходимость использования комплексного и научно обоснованного подхода к обеспечению безопасности Интернета вещей.

Оценка рисков необходима разработчику, чтобы понимать все потенциальные уязвимости. Методология оценки должна охватывать вопросы обеспечения конфиденциальности, безопасности, предотвращения мошеннических действий, кибератак и кражи интеллектуальной собственности. Это отнюдь не простая задача, поскольку киберпреступники находятся в постоянном поиске и постепенно осваивают все новые и новые виды угроз. И поскольку универсального решения для нейтрализации этих угроз не существует, на этом этапе рекомендуется пригласить для консультаций эксперта в области безопасности.

Ключевой момент заключается в том, что безопасность устройства должна учитываться на этапе проектирования. Сюда относится безопасность в конечных точках и профилактические меры, в том числе создание защищенного от взлома аппаратного и программного обеспечения.

Обеспечение безопасности данных достигается путем строгой аутентификации, шифрования и безопасного управления ключами шифрования, которые должны использоваться для защиты информации как хранящейся на устройстве, так и в момент ее передачи.

Управление жизненным циклом подразумевает обеспечение безопасности не как обособленный процесс, который достаточно выполнить один раз и забыть о нем. Крайне важно, чтобы устройства, использующиеся в экосистеме Интернета вещей, были защищены на протяжении всего их жизненного цикла, не важно, идет ли речь о самостоятельном продукте или о некой системе, например, интегрированной в автомобиль.

Таким образом, подводя итог вышеизложенному, отметим, что в соответствии с Доктриной информационной безопасности Российской Федерации (утв. указом Президента РФ от 05.12.2016 № 646) в качестве одной из угроз выделена преступность в кредитно-финансовой сфере. Учитывая повышенный интерес, популярность и распространенность концепции Интернета вещей, следует особое внимание уделить IoT как инновационному методу совершения таких преступлений.

Литература

1. Совместная безопасность: подход к решению проблем интернет-безопасности. Internet Society, апрель 2015 г. URL: https://www.internetsociety.org/ collaborativesecurity.
2. Fiat Chrysler отзывает 1,4 млн машин в США из-за риска взлома хакерами, июль 2015 г. URL: https://ria.ru/world/20150724/1146131999.html.
3. IoT in Financial Services and Banking — Definition and Examples, June 2016. URL: https://www.k-message.com/iot-financial-services-bank-marketing-definition-examples/.
4. Internet of Things: The Complete Reimaginative Force TCS Global Trend Study, July 2015. URL: https://www.tcs.com/SiteCollectionDocuments/White%20Papers/Internet-of-Things-The-Complete-Reimaginative-Force.pdf.
5. *Пол Маккри* (Visa): «Люди не хотят платить, они хотят покупать», август 2016 г. URL: https://bankir.ru/publikacii/20160815/pol-makkri-visa-lyudi-ne-khotyat-platit-oni-khotyat-pokupat-10007916/.
6. Альфа-Банк анонсировал приложение-помощника для финансовых консультаций Sense, сентябрь 2015 г. URL: https://vc.ru/n/alfa-sense.
7. MasterCard представила решения для платежей через холодильник и фитнес-браслеты, январь 2016 г. URL: https://www.banki.ru/news/lenta/?id=8603837.