Александр В. Мамаев[1], Кристина В. Мамаева[2]
[1]ООО «Лаборатория Цифровой Форензики»,
115191, Москва, Духовской переулок, дом 17, пом I ком 2а
e-mail: a.mamaev@forensicservices.ru, http://orcid.org/0000-0002-1216-3486
[2]Национальный Исследовательский Университет «Высшая Школа Экономики»,
101000, г. Москва, ул. Мясницкая, д. 20
e-mail: solnce-tina18@mail.ru, http://orcid.org/0000-0003-0097-799X

КАК ЭКОСИСТЕМА ВИРТУАЛЬНЫХ АССИСТЕНТОВ МОЖЕТ ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

DOI: http://dx.doi.org/10.26583/bit.2018.2.07

Аннотация. Количество преступлений, совершаемых в информационной сфере, постоянно возрастает. Одновременно возрастает совокупный ущерб, наносимый деятельностью киберпреступников: с 1,5 трлн долл. в 2015 году до 2 трлн. долл. к 2019 году. На этом фоне законодательство Европейского Сообщества в области защиты персональных данных, сформированное еще в 1990-е годы, ждут самые кардинальные изменения, что наверняка повлияет на позиции других стран. Персональные данные интернет-пользователей давно превратилось в объект купли-продажи на рынке электронной коммерции. Манипуляции с персональными данными вызывают серьезные возражения со стороны самих пользователей. Власти озабочены сохранностью и конфиденциальностью данных в соответствии с законодательством. Несмотря на это, количество инцидентов, связанных с утечкой или некорректным использованием персональных данных, возрастает по экспоненте: в декабре 2017 года юристы Hill Dickinson подали коллективный иск к Google, недовольные незаконным сбором персональных данных владельцев iPhone. Следом под удар попала компания Uber Technologies, несанкционированно рассылавшая SMS-оповещения клиентам. В марте 2018 года оправдываться за утечку данных 80 млн аккаунтов пришлось соцсети Facebook. Авторы статьи рассмотрели возможности внедрения экосистемы виртуальных ассистентов и технологии блокчейна для безопасной и деперсонализированной обработки персональных данных с последующим использованием, что открывает неожиданные перспективы перед machine-to-machine-marketing.

Ключевые слова: виртуальный ассистент, блокчейн, персональные данные, электронная коммерция.

Для цитирования. МАМАЕВ, Александр В.; МАМАЕВА, Кристина В.. КАК ЭКОСИСТЕМА ВИРТУАЛЬНЫХ АССИСТЕНТОВ МОЖЕТ ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ. Безопасность информационных технологий, [S.l.], n. 2, p. 80-85, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1112>. Дата доступа: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.07.

Alexandr V. Mamaev[1], Kristina V. Mamaeva[2]
[1]CEO at 'Digital Forensics Laboratory LLC',
Dukhovskoy per., 17, bld. I, fl. 2A. 115191, Moscow,Russia
e-mail: a.mamaev@forensicservices.ru, http://orcid.org/0000-0002-1216-3486
[2]National Research University Higher School of Economics,
Myasnitskaya str., 20, 101000, Moscow, Russia
e-mail: solnce-tina18@mail.ru, http://orcid.org/0000-0003-0097-799X

How the ecosystem of digital assistants can ensure the security of personal data

DOI: http://dx.doi.org/10.26583/bit.2018.2.07

Abstract. Number of cybercrimes is constantly rising both in Europe, and around the world. The costs incurred from such malicious activities are rising correspondingly. According to the data collected by Jupiter Research these costs increased from $1.5 trillion in 2015 to $2 trillion in 2019.

That is why European Union is expected to introduce major changes to the Personal Data Protection Acts which stayed mostly unchanged since the 1990s. The consequences of those changes will be felt in countries beyond the European Union. The personal data of internet users have long become a commodity on the e-commerce market. Yet the manipulations with the personal data cause concerns among both the users, who do not fully realize how and to what purposes their data are used, and governments, who try to protect the confidentiality remains by the law. Despite that the number of incidents with data leaks continues to rise exponentially. In December 2017 the lawyers from Hill Dickinson, a UK commercial law firm, filed a lawsuit against Google regarding unlawful collection of the iPhone users' data. Another company that is about to have problems with law is Uber Technologiesm, which sent SMS messages to its clients without obtaining formal permissions for that. Finally, in March 2018 it was Facebook which had to explain the way the personal data on more than 80 million users have leaked and ended up in the hands of a third party. The authors of this article assessed the possibilities for introducing the ecosystem of virtual assistants and blockchain technology for safe and depersonalized data processing as well as its further use. This system opens broad unexpected opportunities for the machine-to-machine-marketing.

Keywords: virtual assistants, blockchain, personal data, e-commerce.

For citation. MAMAEV, Alexandr V.; MAMAEVA, Kristina V.. How the ecosystem of digital assistants can ensure the security of personal data. IT Security (Russia), [S.l.], n. 2, p. 81-86, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1112>. Date accessed: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.07.

На сегодняшний день одной из самых заметных и актуальных проблем является глобальный рост киберпреступности. Согласно данным Juniper Research, совокупный ущерб, наносимый деятельностью киберпреступников, вырастет с 1,5 трлн долл. в 2015 году до 2 триллиона долларов к 2019 году.

Малый и средний бизнес оказался более уязвим для киберпреступников в сравнении с крупными корпорациями. Более 50% предприятий с количеством сотрудников от 100 до 1 тыс. человек подвергались атакам киберпреступников, средний ущерб составил 879,582 долларов США [1].

Рядовые интернет-пользователи не уделяют должного внимания собственной информационной безопасности. Согласно исследованию Symantec, 87% пользователей интернета в США подключались к публичному Wi-Fi без применения дополнительных средств защиты. При этом более 60% респондентов полагали, что их данным ничего не угрожает [2].

Последние пять лет запомнились колоссальным количеством случаев утечек персональных данных, породив серьезные запросы на обеспечение информационной безопасности и вопросы – к руководству компаний, допустивших подобные инциденты. В частности, к самой популярной в мире социальной сети Facebook, которая столкнулась с обвинениями в утечке данных 80 млн пользователей, что серьезно ударило по капитализации компании и пошатнуло позиции топ-менеджмента [3].

Под влиянием общественности и американских властей, инициировавших проверку, корпорация приняла решение изменить систему управления персональных данных и ограничить объем сведений, предоставляемых компаниям сродни Cambridge Analytica, ставшей виновницей разразившегося скандала. Facebook также планирует запретить предоставлять сторонним поставщикам анонимизированные данные пользователей, которые позволяют оценить успешность проводимых рекламных кампаний [4]. Наконец, компания проверит все приложения «с подозрительной активностью» и запретит продолжать деятельность разработчикам, которые откажутся от проведения такой проверки. Все это приведет к тому, что сторонние компании потеряют возможность создавать таргетированную рекламу.

Однако есть куда более простое решение, позволяющее поставить точку в вопросе: устранить личный фактор, передав рекламные кампании в ведение виртуальных

помощников и персональных ассистентов, знающих потребности и запросы своих владельцев. В конечном счете, в основе бизнеса социальных сетей лежит задача электронной коммерции – маркетинг. В интернет-маркетинге ключевая ценность заключается в том, чтобы найти максимальное соответствие между потребностями потенциального покупателя и предлагаемым рекламным контентом. Именно это определяет успешность работы рекламы [5-6].

В настоящее время, маркетинг – это процесс многослойный: сначала специалист формирует требования к портрету покупателя, потом настраивает базовые параметры рекламных кампаний, после чего, в работу вступает информационно-аналитическая машина, которая к этому моменту уже обладает своей базой потенциальных покупателей или может обрабатывать данные из сторонних баз. Итак, такая информационная система будет работать по строгим критериям специалиста, заложенным в рекламной кампании. При этом процесс необходимо постоянно контролировать, вносить регулярные правки и уточнения. Если речь идет о необходимости привлечения большого объема трафика, то процесс будет усложняться, будут применяться дополнительные техники и подходы, например, programmatic.

Как видно, задача «достучаться» до своего покупателя уже сейчас является весьма сложно и трудоемкой. Развитие электронной коммерции, появление новых требований к инструментам, все это только усложнит работу маркетологов. Внедрение machine-to-machine-marketing позволяет выйти из этой ситуации, а также нивелировать угрозы личного фактора.

Данное направление – это результат естественного развития информационного общества и современных технологий. Развитие Интернета вещей приведет к тому, что вокруг человека почти все будет в виде «умного устройства», способного собирать поведенческую информацию о своем пользователе [7]. Другими словами, в скором времени, поведение человека, его привычки, потребности, особенности, ровным счетом абсолютно все будет подвергаться «протоколированию» «умными устройствами» и анализироваться специальными системами [8].

Таким образом, неминуемо пересечение взаимных возможностей интернет-маркетинга и интернета вещей, которое перерастет в новый вид M2M маркетинга, когда участие человека в процессе выбора будет минимально. Виртуальные частные ассистенты начнут самостоятельно принимать решения о выборе того или иного предложения на основании полного портрета своего владельца. Виртуальный ассистент (ВА) - это разговорный, генерируемый компьютером персонаж, который имитирует разговор для предоставления голосовой или текстовой информации пользователю через веб-сайт, киоск или мобильный интерфейс. Виртуальный ассистент может получать команды с помощью ввода текста, голоса или загрузки файла, например, изображения. ВА производят обработку естественного языка, чтобы исполнить команду и выдать ответ [9].

Для реализации в виртуальном ассистенте полноценной системы электронной коммерции необходимо выполнение нескольких условий. Во-первых, должно быть реализовано и поддерживаться сетевое взаимодействие, чтобы обеспечить режим двустороннего взаимодействия. Во-вторых, требуется поддержка технологии блокчейн для того, чтобы процесс взаимодействий был максимально прозрачным и надежным от попыток мошенничества. Рассмотрим по порядку данные требования.

Сетевое взаимодействие. Если не брать в расчет вопросы бизнеса, связанные с постепенным ростом аудитории активных пользователей, то в конечном счете получится новая экосистема виртуальных ассистентов. Это позволит избавить пользователей от большого числа мелких, незначительных действий во взаимодействии с другими людьми. M2M маркетинг - параллельный виртуальный мир, в котором ассистенты выполняют поручения своих владельцев: совершают покупки, обмениваются товарами, услугами, информацией, обеспечивают для своих владельцев непревзойденную доступность возможностей [10].

Система распределенного хранения данных – блокчейн. Одним из важнейших элементов во взаимодействии пользователей в виртуальном мире является вопрос доверия. Если на базе этого реализовывать еще и вопрос торгово-денежных отношений, то задача становится еще важнее. Для решения данной проблемы необходимо использовать такой инструмент, который позволит каждому участнику доверять друг другу при совершении операции [11]. На текущий момент предлагается использовать технологию блокчейна, особый вид хранения данных, при котором каждый новый блок криптографически связан с предыдущем. Для упрощения процессов взаиморасчета будет использована криптовалюта данного виртуального ассистента. Криптовалюта — разновидность цифровой валюты, в основе которой лежит технология блокчейн, а создание и контроль базируются на криптографических методах.

Таким образом, все операции будут реализованы через смарт-контракты, специальный алгоритм, позволяющий в автоматизированном режиме заключать и поддерживать выполнение коммерческих договоров в соответствии с заданными условиями. При этом, каждый участник может лично удостоверится в условиях, алгоритме каждого смарт-контракта и быть уверенным в неизменности и необратимости его действия. Именно это дает уверенность участникам процесса в то, что каждая сторона корректно исполнит свои обязательства.

Рассмотрим теперь, как будет применяться технология виртуального ассистента, изменяя привычную работу социальной сети. Сам механизм становится схожим с работой CPA-сетей, в которых рекламодатели ищут исполнителей в свои программы привлечения клиентского трафика. Однако, в предлагаемой схеме, будет только один вид программы – это продать товар или услугу. Исполнителем, в отличии от CPA-сетей, будет не произвольный «вебмастер», а сама сеть виртуальных ассистентов.

Пример работы ассистентов может выглядеть следующим образом: высокоперсонализированная сеть рекламодателя (например, производитель смартфонов) обращается к площадке (Facebook) с просьбой помочь в продаже 1 млн устройств по заданным параметрам (уровень дохода, предпочтения к марке, сроки оплаты, вплоть до любимого цвета). Соцсеть, не предоставляя заказчику доступа к базе данных, берется за заказ, отправляя таргетированные объявления персональным ассистентам интернет-пользователей.

Для гарантии безопасности и прозрачности всех операций процедура размещения товаров, как и оплата, проходит по технологии блокчейн, фиксирующей все шаги операции и верификации. Таким образом, продавец сможет контролировать путь товара и свою прибыль, посредник (Facebook) снимает с себя все риски перед рекламодателем, а пользователь, подписывая соглашение, дает разрешение на участие в этой схеме. Алгоритм работы предлагаемого механизма представлен на рисунке 1.

Как видно из алгоритма работы, персональные данные пользователей не покидают систему виртуального ассистента. Только в случае приобретения, пользователь сам укажет тот объем информации, минимально необходимый для получения купленного товара или услуги. Эта информация будет передана исполнителю.

Рассмотрим пример того, как виртуальный ассистент будет работать в интересах электронной коммерции, без ущерба для персональных данных пользователя. Описание: пользователь хочет купить обувь. Им уже был проведен предварительный поиск в интернете для определения желаемых параметров. Но покупка не совершена, так как хочется осуществить примерку. Задача: помочь совершить покупку.

На рисунке 2 представлена диаграмма последовательности действий, описывающая процесс решения возникшей задачи.

Как видно из алгоритма работы, персональные данные пользователей не покидают систему виртуального ассистента. Только в случае приобретения, пользователь сам укажет тот объем информации, минимально необходимый для получения купленного товара или услуги. Эта информация будет передана исполнителю.

Рассмотрим пример того, как виртуальный ассистент будет работать в интересах электронной коммерции, без ущерба для персональных данных пользователя. Описание: пользователь хочет купить обувь. Им уже был проведен предварительный поиск в интернете для определения желаемых параметров. Но покупка не совершена, так как хочется осуществить примерку. Задача: помочь совершить покупку.

На рисунке 2 представлена диаграмма последовательности действий, описывающая процесс решения возникшей задачи.

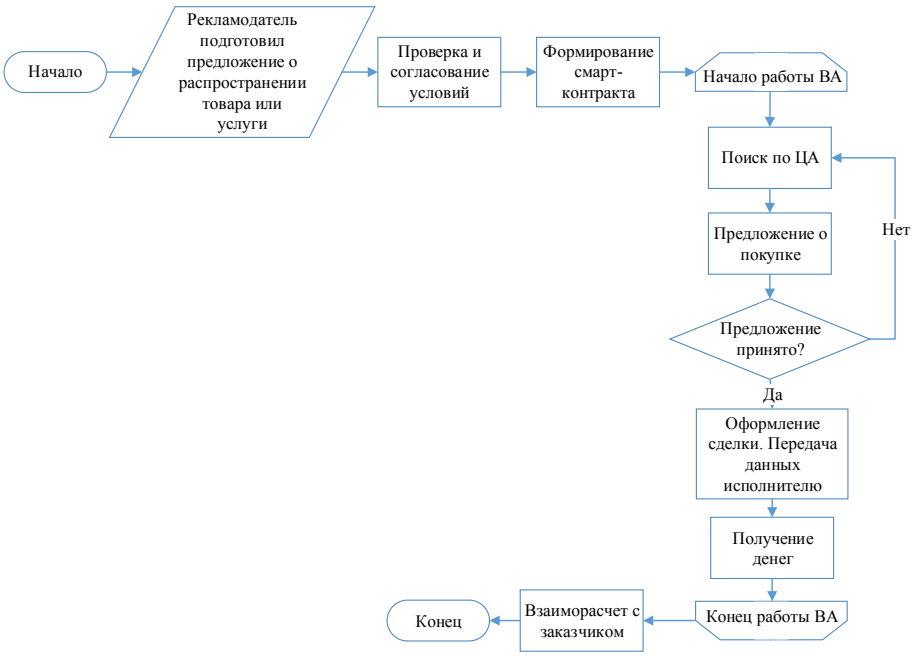

Рис. 1. Алгоритм продажи товаров и услуг через виртуальных ассистентов
(Fig.1. Algorithm for the sale of goods and services through virtual assistants)

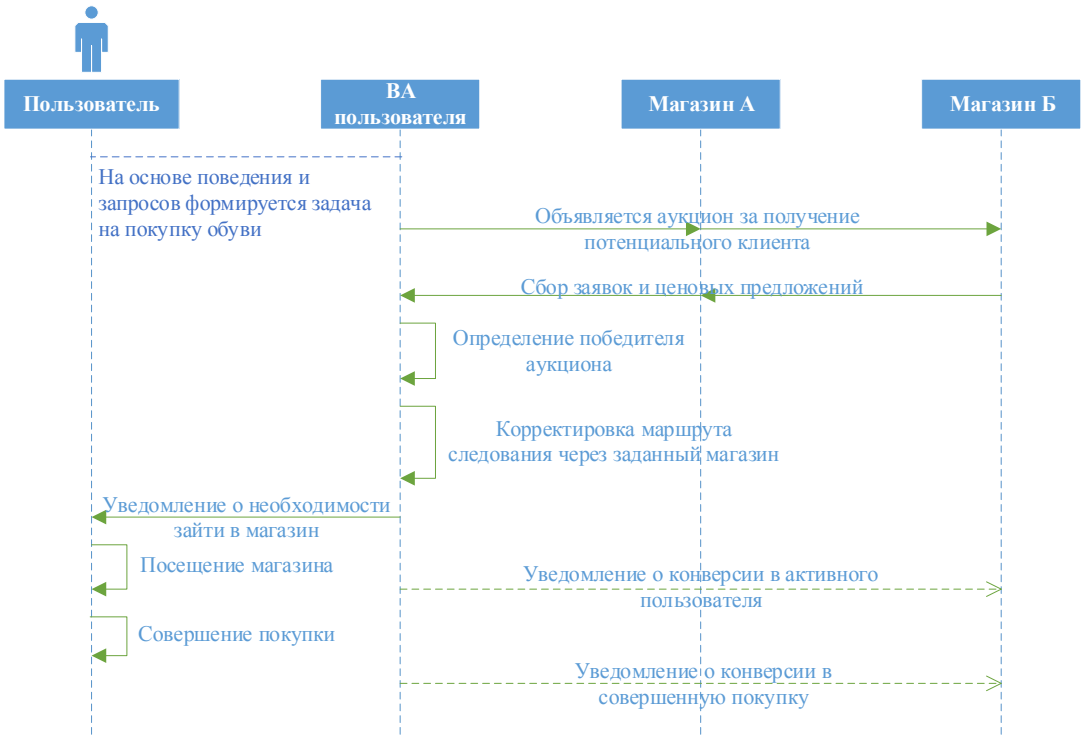

Рис. 2. Диаграмма последовательности действия для рассматриваемого примера
(Fig. 2. Sequence diagram for the example in question)

СПИСОК ЛИТЕРАТУРЫ:

1. The Global Risks Report 2016 [Электронный ресурс] – URL: https://www.weforum.org/reports/the-global-risks-report-2016/.
2. L. Ponemon 2016 Ponemon Institute Cost of a Data Breach Study [Электронный ресурс] – URL: https://securityintelligence.com/media/2016-cost-data-breach-study/.
3. Zuckerberg launches Facebook's Washington defense [Электронный ресурс] – URL: http://www.reuters.tv/v/jqB/2018/04/09/zuckerberg-to-meet-with-lawmakers-ahead- of-hearing.
4. K. Chaykowski Facebook Curbs Information Shared With Data Brokers, Launches New User Privacy Tools [Электронный ресурс] – URL: https://www.forbes.com/sites/kathleenchaykowski/2018/03/29/facebook-to-curb-information- shared-with-data-brokers/#6be4a62fac1a.
5. М.Ю. Наумов, А.С. Чистяков Применение систем искусственного интеллекта в различных сферах деятельности. Постулат. 2017 №5.
6. Glukhov, V.V. Improving the efficiency of architectural solutions based on cloud services integration. V.V. Glukhov, I.V. Ilin, O.J. Iliashenko. Lecture Notes in Computer Science. -2016. -T. 9870. -pp. 512-524.
7. Росляков, А.В. Интернет вещей: учебное пособие [текст]. А.В. Росляков, С.В. Ваняшин, А.Ю. Гребешков. – Самара: ПГУТИ, 2015. – 200 с.
8. McKinsey Global Institute, Digital Globalization: the new era of global flows. Executive Summary, March 2016 .
9. Rob High «Эпоха когнитивных систем: Принцип построения и работы IBM Watson» [Электронный ресурс] – URL: http://www.interface.ru/iarticle/files/36855_77829297.pdf.
10. Unraveling the Hype: AI Marketing Readiness in Retail & E-Commerce [Электронный ресурс] – URL: https://engage.emarsys.com/en/study/ai-readiness (Дата обращения: 15.03.2018).
11. Коршунов Антон Анализ социальных сетей: методы и приложения. Труды ИСП РАН. 2014. №1. [Электронный ресурс] – URL: http://cyberleninka.ru/article/n/analiz-sotsialnyh-setey-metody-i-prilozheniya.

REFERENCES:

[1] The Global Risks Report 2016 [Electronic resource] – URL: https://www.weforum.org/reports/the-global-risks-report-2016/.
[2] L. Ponemon 2016 Ponemon Institute Cost of a Data Breach Study [Electronic resource] – URL: https://securityintelligence.com/media/2016-cost-data-breach-study/.
[3] Zuckerberg launches Facebook's Washington defense [Electronic resource] – URL: http://www.reuters.tv/v/jqB/2018/04/09/zuckerberg-to-meet-with-lawmakers-ahead- of-hearing.
[4] K. Chaykowski Facebook Curbs Information Shared With Data Brokers, Launches New User Privacy Tools [Electronic resource] – URL: https://www.forbes.com/sites/kathleenchaykowski/2018/03/29/facebook-to- curb-information- shared-with-data-brokers/#6be4a62fac1a.
[5] M.Ju. Naumov, A.S. Chistjakov.The use of artificial intelligence systems in various fields. Postulate. 2017 No. 5. (in Russian).
[6] Glukhov, V.V. Improving the efficiency of architectural solutions based on cloud services integration. V.V. Glukhov, I.V. Ilin, O.J. Iliashenko. Lecture Notes in Computer Science. -2016. -T. 9870. -pp. 512-524.
[7] Rosljakov, A.V. The Internet of things: a training manual [text]. A.V. Rosljakov, S.V. Vanjashin, A.Ju. Grebeshkov. – Samara: PGUTI, 2015. – 200 p. (in Russian).
[8] McKinsey Global Institute, Digital Globalization: the new era of global flows. Executive Summary, March 2016.
[9] Rob High «"The era of cognitive systems: the principle of construction and operation of IBM Watson»» [Electronic resource] – URL: http://www.interface.ru/iarticle/files/36855_77829297.pdf . (in Russian).
[10] Unraveling the Hype: AI Marketing Readiness in Retail & E-Commerce [Electronic resource] – URL: https://engage.emarsys.com/en/study/ai-readiness (Date of access: 15.03.2018)
[11] Korshunov Anton. Social media analysis: methods and applications. The proceedings of ISP RAS. 2014. №1. [Electronic resource] – URL: http://cyberleninka.ru/article/n/analiz-sotsialnyh-setey-metody-i-prilozheniya. (in Russian).

Поступила в редакцию – 28 марта 2018 г. Окончательный вариант –23 апреля 2018 г.
Received – March 28, 2018. The final version – April 23, 2018.