чтобы система умела эффективно предвидеть оценки, исходя из небольшого количества примеров. Также необходимо наличие критического количества пользователей [2].

Проблему нового пользователя и проблему нового товара можно решить, используя гибридные подходы к построению рекомендательных систем, совмещая контентные алгоритмы с коллаборативными.

Преодолеть проблему разреженности оценок можно, если при поиске похожих пользователей использовать информацию о пользователе, содержащуюся в его профиле. Это значит, что два пользователя будут считаться похожими не только, если они одинаково оценили одни и те же объекты, но и если они принадлежат к общему демографическому сегменту. Это расширение традиционной коллаборативной фильтрации иногда называется демографической фильтрацией.

В дополнение к традиционным методикам построения потребительского профиля (таким, как опора на ключевые слова и анкетную демографическую информацию) в последнее время появились новые методики, опирающиеся на автоматическую обработку текстов (data – mining), анализ сетевого поведения и т.д. Эти методики позволяют учесть интересы и предпочтения пользователей и тем самым расширить пользовательский профиль.

Список использованных источников

1. Francesco Ricci; Lior Rokach; Bracha Shapira; Paul B. Kantor, ed. Recommender Systems Handbook. Springer, ISBN 978-0-387-85819-7.

2. Adomavicius, Gediminas. Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions. Gediminas Adomavicius, Alexander Tuzhilin, IEEE TRANSACTIONS 73ON KNOWLEDGE AND DATA ENGINEERING. — 2005. — Vol. 17, no. 6. — Pp. 734–749.

УДК 004

РИСКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И «ИНТЕРНЕТ ВЕЩЕЙ»

Хрипович И.С.

Учреждение БГУ «Научно-исследовательский институт прикладных проблем математики и информатики»

E-mail: hripovich@bsu.by

Abstract. *INFORMATION SECURITY RISKS AND INTERNET OF THINGS. Internet of Things is a future-facing development of the internet wherein objects and systems are embedded with sensors and computing power, with the intention of being able to communicate with each other. There are many information security risks grows up with this technologies and the traditional risk management approach, which assumes that the trust boundary is already defined, can't respond for modern challenges.*

Аннотация: *«Интернет вещей» является перспективной концепцией глобальной сети, объединяющей объекты и системы, имеющие встроенные сенсоры и вычислительные ресурсы, с возможностью взаимодействия. С повсеместным внедрением данных технологий связан существенный рост рисков информационной безопасности. Традиционный подход к управлению риском основывается на определении границы доверия и не может эффективно решать возникающие задачи.*

Основной текст:

Концепция «Интернета вещей» базируется на повсеместном внедрении следующих технологий: беспроводные сети, облачные вычисления, межмашинное взаимодействие. Данная концепция набирает популярность, потому что направлена в первую очередь на повышение

комфорта каждого человека. Начиная от смартфона, который может проверять почту и сигнализировать о новых сообщениях в соцсетях и заканчивая беспилотным автомобилем.

На сегодняшний день одной из основных проблем, связанной с «Интернетом вещей» является отставание теоретического базиса от практической реализации. С течением времени данный разрыв не уменьшается, а только увеличивается, прежде всего, речь идет о стандартизации используемых технологий и их совместного применения. В свою очередь стандартизация невозможна без полноценной оценки рисков.

По мере того как «Интернет вещей» всё больше проникает в повседневную жизнь людей, растут и динамично изменяются риски информационной безопасности, с ним связанные. В реалиях современного информационного пространства риски информационной безопасности актуальны для всех пользователей и угрозы переходят из класса «если» в класс «когда».

Информационная безопасность является задачей уровня организации и даже уровня государства, а не ограничивается рисками информационных технологий. Традиционные модели управления риском базируются на предположениях, что организация имеет достаточный контроль над своими активами, в частности: есть контролируемая зона в которой располагается оборудование и хранятся данные, определены каналы взаимодействия активов организации с внешними субъектами. Однако девизом современных технологий является стирание границ и мобильность. Пользователь хочет иметь возможность получения доступа к сервису в любое время с любого устройства и из любой точки земного шара. При этом речь идет не только о привычных публичных сервисах. Под сервисом в данном контексте может пониматься получение доступа к рабочему месту, или базам данных, расположенным в облачном вычислительном центре.

Таким образом, система управления рисками информационной безопасности должна покрывать всю экосистему организации: непосредственно активы организации, клиентов, потребителей, поставщиков, партнеров. Большая часть перечисленных субъектов находится вне контроля организации, зачастую они имеют собственные политики в области информационной безопасности, которые могут противоречить приоритетам организации. Традиционные подходы к оценке риска определяют границу доверия и внедрение новых технологий, процессов, политик приводит к расширению этой границы.

«Интернет вещей» предполагает прозрачное взаимодействие человека и всех устройств, что его окружают, а также этих устройств между собой и с внешними сервисами. Под внешними сервисами подразумеваются как коммерческие, так и государственные сервисы, например, вызов такси, заказ пиццы, но и вызов скорой помощи, милиции, службы спасения.

С точки зрения технологий наиболее критичными направлениями в контексте «Интернета вещей» являются идентификация субъектов, доверенные каналы передачи данных и доверенные источники данных. Данные направления достаточно хорошо изучены и реализованы соответствующие механизмы защиты.

С точки зрения информационной безопасности «Интернет вещей» несет в себе риски связанные в первую очередь с личными данными человека, концепция «Интернета вещей» подразумевает не только доступность сервисов человеку, но и доступность данных о человеке для сервисов. Сенсоры в «умном доме» отслеживают передвижение человека по дому и корректируют освещение, служба такси при вызове получает данные о местоположении от смартфона, с которого осуществляется вызов, «умные часы» контролируют пульс и могут вызвать «скорую», если человеку станет плохо, браузер собирает информацию о страницах, которые посещал человек, навигатор в автомобиле запоминает маршруты, по которым он ездил. Вся эта информация накапливается и предоставляется различным сервисам, облегчающие жизнь человека. Добавление к этим данным сведений о банковских реквизитах, медицинских данных формирует достаточно полное досье на человека. Таким образом, проблемы информационной безопасности «Интернета вещей» становятся задачей государственной важности, требующей всесторонней оценки и анализа.