Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

Одним из первых решений данного подхода были системы, основанные на большом количестве правил *регулярных выражений* (RegEx), суть ее заключалась в следующем: использую синтаксис регулярных выражений, создавались специальный шаблон, по которому находятся совпадения в тексте, например - шаблон для поиска email адреса в тексте:

Фактически, задача сводится к разработке анализатора названия музыкальной композиции.

Таким образом, актуальными являются исследования, связанные с разработкой информационных систем для анализа информации из сети Интернет.

Список литературы

1. Официальная документация проекта Apache OpenNLP – Режим доступа: https://opennlp.apache.org/documentation/1.5.3/manual/opennlp.html.

2. ГОСТ Р 7.0.8-2013. Делопроизводство и архивное дело. термины и определения.

3. Проект лингвистического корпуса Пенсильванского университета, [Электронный ресурс] режим доступа: http://www.cis.upenn.edu/~treebank/.

4. Обработка неструктурированных текстов - Грант Ингерсолл и др. ДМК-пресс, 2013.

5. О.В. Пескова, "Методы автоматической классификации текстовых электронных документов", ISSN 0548-0027, НТИ, Сер.2, Информ. процессы и системы, 2006, №3.

ПРОБЛЕМЫ СТАНДАРТИЗАЦИИ И БЕЗОПАСНОСТИ «УМНЫХ» СИСТЕМ

И.Д. КОТИЛЕВЕЦ

Московский технологический университет

В последние годы стала популярна концепция технологий, известных как «умный дом», «умный город», направленных на автоматизацию, ресурсосбережение, улучшение жизни. Но пока эти понятия практически никак не связаны, синергия направлена исключительно внутрь систем, из-за чего затруднено развитие инфраструктуры, жилищно-коммунального хозяйства и других служб на уровне самого города, муниципалитета и на уровне домов. Не происходит интеграции «умного дома» с «умным городом». Появляются лишние или избыточные службы или узлы, перерасход ресурсов, а также проблемы с безопасностью.

В связи с этим в настоящее время становится актуально создание стандарта проектирования систем «умных домов» для непосредственной интеграции в «умный город».

Умный дом. В основе как «умного города», так и «умного дома» лежит «интернет вещей» (IoT), объединяющий множество устройств самого разного назначения.

Поскольку система «умный дом» является разновидностью промышленной автоматизации, то универсальные настраиваемые средства могут быть основополагающими элементами для организации всего процесса управления с переходом от несвязанных подсистем к полной автоматизации и связям с высокоуровневыми приложениями вплоть до формирования отчетов о потребленных ресурсах [1, 2].

На сегодняшний день в мире разработаны и внедрены сотни таких систем. Но, во-первых, они малоприменимы в России без адаптации, так как разработаны с учётом западных или американских стандартов управления. Во-вторых, на данный момент практически не существует поддержки подобных решений в России – автоматизация является длительным и трудоемким процессом, требующим постоянного участия предметного специалиста, разработчика и поставщика оборудования [3].

Это осложняется одной из главных проблем — отсутствием стандартизации при разработке «умных домов». Каждый производитель использует свой подход к реализации систем. Это касается как проводных решений, например, KNX, так и беспроводных систем. В итоге в одном многоквартирном доме могут существовать экосистемы различных «умных домов», что может повлечь за собой сбои оборудования или выход из строя отдельных устройств IoT.

При этом далеко не все производители озаботились безопасностью в сфере IoT, частью которой является и «умный дом». Взлом камер наблюдения, дверей и освещения представляет собой потенциальную опасность кражи материальных ценностей или данных. Даже взлом умного холодильника позволяет хакерам украсть пользовательский пароль аккаунта Google. Но критически важным становится взлом устройств, от которых зависит жизнь людей. Не так давно один хакер взломал инсулиновую помпу, другие – бортовой компьютер автомобиля. Это дает возможность ввести человеку смертельную дозу инсулина или отключить тормоза, спровоцировав смерть людей, и при этом остаться безнаказанным. Проблема безопасности «умных» вещей – одна из основных на сегодня. «Умная» техника – наиболее уязвимая технология с точки зрения интернет-угроз [4-7].

Умные города. Понятие «умный город» в последнее время стало применяться к семейству технологий, способных ускорить развитие города, повысить эффективность всех городских служб и качество жизни в нем. Это подразумевает, например, грамотное и экономичное распределение ресурсов, эксплуатационных издержек, увеличение безопасности, предотвращение аварийных ситуаций.

Перечень областей, которые требуют внедрения умных технологий, охватывает практически все без исключения сферы городского хозяйства и городской инфраструктуры.

В настоящий момент создано более 2000 «умных городов» в том или ином виде. Можно сказать, что именно из-за масштабного применения различных информационных технологий такого рода проекты всегда будут одними из самых крупных [8,9].

Чтобы город считался умным, он должен предоставлять базовые элементы для реализации сервисов Типичный пример объединения различных «умных» технологий, имеющий прямое отношение к теме «умных городов» – это HyperCat. В России также существуют несколько проектов умных городов, часть функций «умных городов» уже внедряются в города-миллионники Отдельно можно упомянуть Иннополис – «умный город» в Татарстане [10-12].

Несмотря на развитие «умных» технологий, проблемы у «умных городов» такие же, как и у «домов» – отсутствие единого стандарта и интеграции с некоторыми подсистемами, большая вероятность взлома устройств. Учитывая масштабы IoT в таком городе, взлом даже нескольких устройств может повлечь за собой катастрофу.

Таким образом, при разработке «умных» технологий следует обратить особое внимание на защиту от несанкционированного доступа к устройствам Интернета Вещей. Чтобы защитить IoT, предлагается использовать технологию блокчейн [13, 14].

В блокчейне можно хранить данные о выданных кредитах, правах на собственность, нарушении правил дорожного движения, бытовых счетчиков. Одной из особенностей блокчейна является прозрачность всех проводимых транзакций и множественное копирование этих транзакций таким образом, что у каждого участника процесса всегда есть информация о каждом шаге всех партнеров.

Это обеспечивает должный уровень открытости сделок — вся цепочка транзакций дублируется и хранится в неизменном зашифрованном виде у каждого участника сделки. Ее не получится подделать. Более того, участники сделки могут быть как анонимными, так и идентифицированными в зависимости от самой платформы, где проводилась сделка, и цели ее создания и использования.

Также неоспоримым преимуществом является то, что этот реестр не хранится в каком-то одном месте. Он распределён среди нескольких сотен и даже тысяч компьютеров во всем мире. Любой пользователь может иметь свободный доступ к актуальной версии реестра, что делает его прозрачным абсолютно для всех участников.

Блокчейн децентрализован, нет какого-то единого “центрального сервера”, взломав который получится уничтожить все данные о сделке и ее участниках или подменить их. Благодаря данной технологии можно снизить вероятность взлома или неправильной эксплуатации устройств в «умном доме» или «умном городе», устранить лишние связи или службы, сэкономить ресурсы или предотвратить аварию.

Список литературы

1. Максименко В.А. «Интеллектуальное здание»: автоматизированная система диспетчерского управления // СтройПРО ФИль. – 2003. – № 5. – С. 20.

2. Соловьев М.М. Интеллектуальное здание. Понятия и принципы // Строительная инженерия. – 2005. – № 3. – С. 10.

3. Намиот Д.Е., Куприяновский В.П., Синягов С.А. Инфокоммуникационные сервисы в умном городе// International Journal of Open Information Technologies vol. 4, no. 4, 2016.

4. Американский программист взломал свою инсулиновую помпу [Электронный ресурс] / – Режим доступа: http://medportal.ru/mednovosti/news/2011/08/05/pumphack/, свободный. – Загл. с экрана.

5. Глупые ошибки умных домов [Электронный ресурс] / – Режим доступа: https://blog.kaspersky.ru/study-smart-homes-insecure/4030/, свободный. – Загл. с экрана.

6. Как взламывают умную технику и как ее защитить [Электронный ресурс] / – Режим доступа: http://ichip.ru/kak-vzlamyvayut-umnuyu-tekhniku-i-kak-ee-zashhitit.html, свободный. – Загл. с экрана.

7. Гатиятуллин Т.Р., Круцких Т.К. Проблемы безопасности Smart TV. Символ науки. Выпуск № 1-2 / 2016.

8. Намиот Д.Е. Умные города 2016 //International Journal of Open Information Technologies. – 2016. – vol. 4. – №. 1.

9. Намиот Д.Е., Шнепс-Шнеппе М. On IoT Programming //International Journal of Open Information Technologies. – 2014. – Т. 2. – №. 10. – С. 25–28.

10. Urban Platforms. [Электронный ресурс] / Электрон. Дан. – Берлин – 2016 – Режим доступа: https://eu-smartcities.eu/content/urban-platforms, свободный. – Загл. с экрана.

11. Hypercat [Электронный ресурс] / Электрон. Дан. – Лондон – 2014 – Режим доступа: http://www.hypercat.io/, свободный. – Загл. с экрана.

12. «Умный город» XXI века: в России начали строить электродома [Электронный ресурс] /Электрон. Дан. – Москва – 2015 – Режим доступа: https://realty.rbc.ru/news/58173f3e9a7947a39ea5fb7a, свободный. – Загл. с экрана.

13. Сирануш Ш.Б. Блокчейн: внезапно нужен всем [Электронный ресурс] / Ш.Б. Сирануш. – Режим доступа: .http://www.rbc.ru/magazine/2016/01/56ba1b779a79477d693621e7, свободный. - Загл. с экрана;

14. Что такое блокчейн и зачем он нужен [Электронный ресурс] /– Москва – 2017 – Режим доступа: https://habrahabr.ru/company/bitfury/blog/321474/, свободный. – Загл. с экрана.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА В КОНТЕКСТЕ БОЛЬШИХ ДАННЫХ

В.А. КУРБАЦКИЙ

Белорусский Государственный Университет

В докладе рассматриваются основные принципы обеспечения Личной Информационной Безопасности с учетом влияния больших данных в условиях современного кризиса информационной безопасности, предлагается концептуальный подход и концептуальная архитектура Личной Информационной Системы со встроенным средством персональной защиты информации «защищенный криптоконтейнер».

Человек стремительно погружается в киберпространство, ведет в нем бизнес, финансовые операции, активно получает образовательные и другие социальные услуги. При этом уже становится очевидным, что эти процессы приводят к формированию Больших данных, связанных с человеком. Возникает вопрос: так ли это безопасно для человека? И обеспечиваем ли мы безопасную среду личного информационного пространства в должной мере? Очевидна потребность в исследовании способов защиты личного информационного пространства и разработке перспективных средств обеспечения личной информационной безопасности с учетом влияния Больших данных. Мы привыкли думать, что знаем больше, чем знаем на самом деле. Наше понимание эффектов технологии отстает от неумолимых последствий ее применения на десятилетия [1].

Всегда ключевым являлось понимание важности связей между людьми. Сейчас к этому добавляется еще и следующее. Связь людей и умных устройств со множеством встроенных механизмов сбора пользовательских данных оказывает огромное влияние практически на все современные сферы общественной жизни, предоставляя потенциально широкие возможности для прогнозирования. Дело в том, что единожды собранные данные, в современных условиях могут храниться практически неограниченное время и быть подвергнуты повторному анализу с приходом новых, более совершенных аналитических алгоритмов, уточняя результаты прогнозирования и открывая новые, до этого невидимые, свойства. Это означает, что все больше средств будет вкладываться в инструменты сбора и анализа Больших данных, а тема безопасности Личного Информационного Пространства будет становиться все актуальнее [2].

Системы сбора и анализа Больших данных должны основываться на тщательно обдуманных принципах, с учетом необходимости защищать частную жизнь и гражданские свободы, с учетом того факта, что эти системы создаются по определенным правилам. Однако, правила, создаваемые людьми, со всеми их изъянами и недостатками, иногда порождают аномалии с невообразимым исходом. Не стоит питать надежд, что одних лишь нормативно-правовых мер и стандартизации хватит для того, чтобы обезопасить человека от возможных рисков Личной Информационной Безопасности.

Одна из основных проблем безопасности информации заключается в том, что при интенсивном развитии информационно-коммуникационных технологий существует ощутимый недостаток времени и ресурсов для экспертной оценки тех или иных программных продуктов (средств хранения, обработки и передачи данных; протоколов и т.д.) и выработки эффективной стратегии защиты информации (как персональной, так