БЕЗОПАСНОСТЬ МОБИЛЬНОЙ КОММЕРЦИИ

Совершать покупки, переводить деньги, идентифицировать личность, используя мобильные или носимые устройства, стало возможным благодаря распространению технологии беспроводной связи малого радиуса действия, или технологии коммуникации ближнего поля (Near Field Communication / NFC). В перспективе ближайших 5 лет она дает большой стимул для развития мобильной коммерции и постепенного отказа от банковских карт в пользу смартфонов. Однако даже когда мобильные устройства просто включены и не используются напрямую, существуют потенциальные угрозы перехвата и манипуляции финансовой информацией.

Во избежание утечки данных и несанкционированных транзакций во время бездействия мобильного устройства, конфиденциальная информация может физически храниться в облачных сервисах с помощью технологии HCE (Host Card Emulation) и ее аналогах.

Для обработки платежной информации и шифрования транзакций используется микрочип Secure Element (SE), внедряемый в мобильное или любое другое устройство с технологией NFC. В отсутствие задач он может выключаться.

ТЕХНОЛОГИЧЕСКАЯ ЭВОЛЮЦИЯ: БЕСПРОВОДНАЯ СВЯЗЬ МАЛОГО РАДИУСА ДЕЙСТВИЯ NFC

ЭФФЕКТЫ

Сокращение киберкраж и других махинаций.

Развитие мобильной коммерции.

Потенциал использования технологий дополненной реальности в магазинах, а также появления виртуальных магазинов с тэгами NFC вместо физических продуктов.

Снижение значимости наличных денег.

Интеграция функций банковских карт, различных пропусков и других магнитных устройств в мобильном телефоне.

ОЦЕНКИ РЫНКА

$21,84 млрд

может составить рынок NFC к 2020 году (при ежегодном темпе роста в 17,1%), а оборот платежей, осуществляемых с помощью телефонов, поддерживающих NFC, превысит 130 млрд долларов в год. Наибольшая доля рынка сейчас принадлежит США, однако самый высокий темп роста прогнозируется для Азиатско-Тихоокеанского региона.

Вероятный срок максимального проявления тренда: 2016–2025 гг.

ДРАЙВЕРЫ И БАРЬЕРЫ

↑ Развитие беспроводных технологий коммуникации ближнего поля действия.

↑ Рост числа услуг, оплачиваемых онлайн с помощью мобильных устройств, массовый переход к электронной и мобильной коммерции.

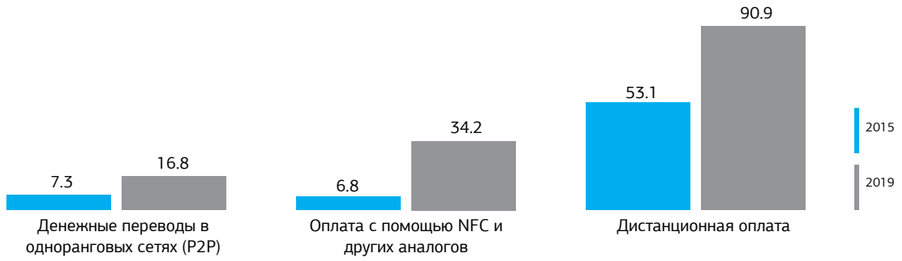
↑ Высокий уровень производительности современных смартфонов, планшетов и носимых устройств.

⊘ Сформированные стереотипы относительно оплаты товаров и услуг с помощью банковских карт или наличными.

⊘ Опасность сосредоточения всей важной финансовой и личной информации на одном устройстве ввиду его возможной потери или кражи.

⊘ Недоверие к облачным сервисам с точки зрения хранения зашифрованной финансовой информации.

СТРУКТУРНЫЙ АНАЛИЗ: Прогноз перехода покупателей на разные виды оплаты с помощью мобильных устройств в США (млрд долларов)



МЕЖДУНАРОДНЫЕ НАУЧНЫЕ ПУБЛИКАЦИИ

МЕЖДУНАРОДНЫЕ ПАТЕНТНЫЕ ЗАЯВКИ

УРОВЕНЬ РАЗВИТИЯ ТЕХНОЛОГИИ В РОССИИ

«Возможность альянсов»: наличие отдельных конкурентоспособных коллективов, осуществляющих исследования на высоком уровне и способных «на равных» сотрудничать с мировыми лидерами

ГЛОБАЛЬНЫЕ ТЕХНОЛОГИЧЕСКИЕ ТРЕНДЫ
HTTP://ISSEK.HSE.RU/TRENDLETTER ТРЕНДЛЕТТЕР #18 • 2015

ИНФОРМАЦИОННО КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

ЗАЩИТА ДАННЫХ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ

Многие быстрорастущие рынки связаны с передачей через беспроводные каналы больших объемов данных от различных устройств: сенсоров, смартфонов, часов, термостатов, холодильников. Причем информация может иметь отношение к здоровью (персонализированная медицина), деньгам (мобильная коммерция), жилищу («умные» дома) и т.п. Для ее передачи требуются надежные стандарты и технологии защиты.

Между тем, например, далеко не во всех представленных на рынке мобильных и носимых устройствах мониторинга спортивной активности и показателей здоровья передаваемые данные защищены должным образом. В частности, не во всех решениях еще используются алгоритмы шифрования. Как и не все пользователи хорошо подкованы в вопросах защиты персональных данных. На фоне роста популярности интеллектуальных услуг развиваются новые криптографические схемы, нацеленные на поиск ошибок, упущений и недоработок программных решений и архитектуры. Отсутствие своевременного реагирования на новые вызовы грозит взломами информационных систем и массовыми махинациями с персональными данными.

Предотвратить эти угрозы помогут стандартизация протоколов беспроводной передачи данных в распределенных сетевых инфраструктурах, использование гомоморфных алгоритмов шифрования информации, а также содержание зашифрованных пакетов данных в облачных сервисах.

В настоящем выпуске информационного бюллетеня представлены перспективные на горизонте ближайших пяти лет технологические решения для безопасной передачи финансовых, медицинских и других персональных данных и защиты «умных» инфраструктур от несанкционированного воздействия.

Трендлеттер выходит 2 раза в месяц.

Каждый выпуск посвящен одной теме:

– Медицина и здравоохранение
– Рациональное природопользование
– Информационно-коммуникационные технологии
– Новые материалы и нанотехнологии
– Биотехнологии
– Транспортные средства и системы
– Энергоэффективность и энергосбережение

В следующем номере:

Медицина и здравоохранение

Мониторинг глобальных технологических трендов проводится Институтом статистических исследований и экономики знаний Высшей школы экономики (issek.hse.ru) в рамках Программы фундаментальных исследований НИУ ВШЭ.

При подготовке трендлеттера использовались следующие источники: Прогноз научно-технологического развития РФ до 2030 года (prognoz2030.hse.ru), материалы научного журнала «Форсайт» (foresight-journal.hse.ru), данные Web of Science, WIPO, PwC, Juniper Research, marketsandmarkets.com, nearfieldcommunication.org, vc.ru, silabs.com, iotevolutionworld.com, ixbt.com, ibtimes.co.uk, prweb.com, globenewswire.com, cybersecuritydojo.com, Icontrol Networks, и др.

Более детальную информацию о результатах исследования можно получить в Институте статистических исследований и экономики знаний НИУ ВШЭ: issek@hse.ru, +7 (495) 621-82-74.

Над выпуском работали: Павел Бахтин, Вероника Ефименко, Анна Соколова, Елена Гутарук, Ким Воронин.

ГОМОМОРФНОЕ ШИФРОВАНИЕ МЕДИЦИНСКИХ ДАННЫХ

Показатели частоты сердцебиения, температуры, дыхания, кровяного давления, уровня глюкозы и другую персональную информацию о пациенте определяют устройства для мониторинга состояния здоровья (носимые или вживляемые). Эта информация может сразу передаваться в лечебные учреждения по сети или через беспроводные каналы связи. Какое-либо вмешательство в процесс передачи данных опасно для пациента не только в связи с возможностью утечки третьим лицам (например, с целью извещения страховых организаций), но особенно в случае их изменения. Так, не зная, что статистика искажена, врач поставит неверный диагноз, а устройства персонализированной медицины подадут лекарства в такой дозе, которая может нанести прямой вред здоровью.

Гомоморфное шифрование медицинских данных, когда они передаются отдельными зашифрованными пакетами через независимые линии связи, решает проблему безопасности. Финальное объединение пакетов, в результате которого информация также остается в зашифрованном виде, происходит на медицинском сервере, что делает бессмысленным перехват отдельных частей во время передачи. На этапе получения данных в медицинском учреждении их целостность и неизмененный характер проверяют с помощью кода аутентификации сообщения (message authentication code / MAC). Ключ для расшифровки данных есть только у лечащего врача или, в случае персонализированной медицины, на устройстве подачи лекарств, что блокирует доступ к информации другим медицинским работникам или хакерам.

ТЕХНОЛОГИЧЕСКАЯ ЭВОЛЮЦИЯ: БЕЗОПАСНОСТЬ И БЕСПРОВОДНЫЕ ТЕХНОЛОГИИ ДЛЯ МЕДИЦИНСКИХ УСТРОЙСТВ

ЭФФЕКТЫ

Рост доверия населения к носимым и вживляемым устройствам мониторинга показателей здоровья.

Развитие сферы дистанционного медицинского мониторинга, стандартизация лечебных услуг.

Создание безопасной распределенной сетевой инфраструктуры передачи медицинских данных.

Распространение технологий персонализированной медицины.

ОЦЕНКИ РЫНКА

$ 7,8 млрд

может достичь к 2020 году мировой рынок носимых медицинских приборов при среднем темпе роста 15% в год (в 2014 году эксперты оценивали объем этого рынка в 3,5 млрд долларов).

Более 200 миллионов носимых устройств в мире будут использоваться к 2018 году.

Вероятный срок максимального проявления тренда: 2018–2030 гг.

ДРАЙВЕРЫ И БАРЬЕРЫ

↑ Распространение мобильных, носимых и вживляемых устройств мониторинга физической активности и показателей здоровья.

↑ Развитие безопасных энергоемких биодеградируемых беспроводных сенсоров и имплантов.

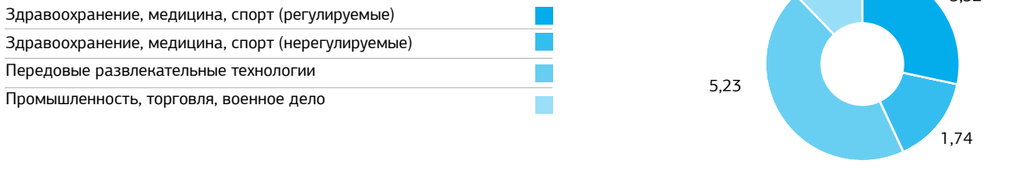
↑ Высокая смертность населения от болезней сердечно-сосудистой системы, высокого давления, диабета, рака и других хронических заболеваний, требующих постоянного контроля.

⊘ Сложность систем безопасности, недостаточная осведомленность об их использовании среди населения.

⊘ Недоверие людей к хранению и передаче конфиденциальных данных, касающихся здоровья, а также к персонализированной медицине.

⊘ Высокая стоимость внедрения инфраструктуры дистанционного мониторинга.

СТРУКТУРНЫЙ АНАЛИЗ: МИРОВОЙ РЫНОК НОСИМЫХ УСТРОЙСТВ ПО СЕГМЕНТАМ В 2015 ГОДУ (МЛРД ДОЛЛАРОВ):



МЕЖДУНАРОДНЫЕ НАУЧНЫЕ ПУБЛИКАЦИИ

МЕЖДУНАРОДНЫЕ ПАТЕНТНЫЕ ЗАЯВКИ

УРОВЕНЬ РАЗВИТИЯ ТЕХНОЛОГИИ В РОССИИ

«Заделы» — наличие базовых знаний, компетенций, инфраструктуры, которые могут быть использованы для форсированного развития соответствующих направлений исследований.

ЗАЩИТА ИНФОРМАЦИИ В «УМНЫХ» ДОМАХ

Инженерные системы «умного» дома обеспечивают постоянный мониторинг и оптимизацию использования всех ресурсов (воды, отопления, электричества), защищают от проникновения злоумышленников, утечки газа, пожара и предупреждают о других чрезвычайных ситуациях. Расположенные в доме устройства связаны как между собой, так и с внешними центрами обработки данных поставщиков услуг, и между всеми ними по беспроводным каналам идет обмен конфиденциальной информацией. В случае ее утечки жилые здания могут стать уязвимыми для несанкционированного проникновения и выведения из строя интеллектуальных систем.

Защиту персональных данных в интеллектуальных системах «умного» дома обеспечивает распределенная инфраструктура сети. Она стандартизирует протоколы обмена и шифрования данных, поступающих от различных сенсоров, камер слежения, бытовых приборов и иных устройств. Это позволяет поставщикам услуг их однозначно идентифицировать с помощью меток (например, RFID, NFC). Приборы соединяются с домашним шлюзом передачи данных, связанным со станцией обработки данных поставщика напрямую через защищенный межмашинный протокол. Для контроля этой системы (ввода паролей, отправки команд) и получения оповещений от поставщика услуг используется мобильный телефон или другое носимое устройство.

ТЕХНОЛОГИЧЕСКАЯ ЭВОЛЮЦИЯ: ЭТАПЫ РАЗВИТИЯ «УМНЫХ ДОМОВ»

ЭФФЕКТЫ

Снижение рисков чрезвычайных ситуаций в жилых зданиях.

Снижение уязвимости «умных» домов от внешних сетевых атак и попыток перехвата персональных данных.

Развитие «Интернета вещей» и спроса на «умные» технологии для домашнего применения.

Появления новых бизнесов и услуг доставки продуктов на основе данных «умных» холодильников и других устройств.

ОЦЕНКИ РЫНКА

$34 млрд

может достичь к 2020 году рынок систем автоматизации «умных» домов при среднегодовом темпе роста в 21%. К 2022 году в доме с полной семьей может использоваться в среднем до 500 «умных» устройств. Основные игроки на рынке защиты систем «умного» дома: Siemens AG (Германия), Schneider Electric S.A. (Франция), ABB Ltd. (Швейцария).

ДРАЙВЕРЫ И БАРЬЕРЫ

↑ Развитие сенсорных технологий, систем контроля и автоматизации.

↑ Широкое распространение сети Интернет и мобильных устройств.

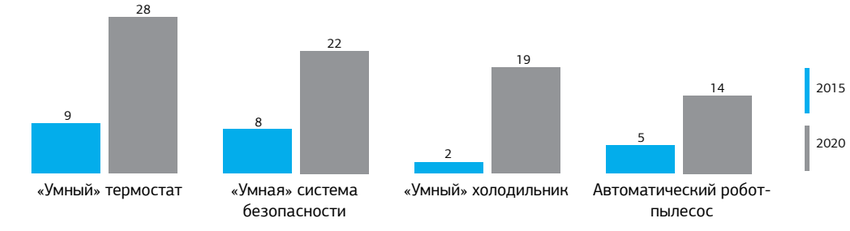
↑ Развитие электронного бизнеса, в частности услуг доставки.

⊘ Сложность использования систем безопасности.

⊘ Недоверие к автоматическому управлению домом.

⊘ Высокая стоимость внедрения и поддержки «умной» инфраструктуры с технической и организационной точек зрения.

СТРУКТУРНЫЙ АНАЛИЗ: ПРОГНОЗ ПЕРЕХОДА ПОКУПАТЕЛЕЙ НА «УМНЫЕ» УСТРОЙСТВА ДЛЯ ПРИМЕНЕНИЯ В БЫТУ (% ОТ ОБЩЕГО ЧИСЛА ПОТРЕБИТЕЛЕЙ)



МЕЖДУНАРОДНЫЕ НАУЧНЫЕ ПУБЛИКАЦИИ

МЕЖДУНАРОДНЫЕ ПАТЕНТНЫЕ ЗАЯВКИ

УРОВЕНЬ РАЗВИТИЯ ТЕХНОЛОГИИ В РОССИИ

«Возможность альянсов»: наличие отдельных конкурентоспособных коллективов, осуществляющих исследования на высоком уровне и способных «на равных» сотрудничать с мировыми лидерами