CIS
Современные Информационные Системы
№ 1 (7) / 2019

Мотивация ИТ-специалистов

Стр. 16

Рынок труда

Алиса

Стр. 4

Искусственный интеллект

Схема движения к цифровой экономике

Стр. 24

ПЯТЬ ГЛАЗ Большого Брата

Стр. 8

Клептография от ОСВ-II до наших дней

ПРЕДИСЛОВИЕ

ТЕХНОЛОГИИ

РЕШЕНИЯ

ОПЫТ

ЭКОНОМИКА

ПРОДУКТЫ

КУЛЬТУРА

ФОТООТЧЁТ

КРОССВОРД

КАЛЕНДАРЬ

От редактора

В этом номере мы поговорим о таком термине, как «цифровая трансформация», который помогает эффективно продвигать большой спектр идей и технологических решений. Достаточно подробно разберём тему шифраторов, которые применяются для построения городских и глобальных сетей.

Проследим за историей клептографии от OCB-II до наших дней и сделаем обзор на тему искусственного интеллекта, попытаемся понять, насколько эта технология востребована в будущем и что она нам сулит.

Приведём прогнозы и статистик по рынку труда, где было проведено исследование «Мотивация ИТ-специалистов», которое поможет работодателям узнать, чего же на самом деле хотят сотрудники ИТ-сферы.

Теперь в журнале есть новая рубрика «Культура», где мы будем рассказывать и показывать актуальные тренды современного медиа- и технологического искусства, а также смежных пространств творческого высказывания.

Мы рады поделиться с вами ещё одной новостью: наша редакция организовала всероссийский ежегодный конкурс красоты «Мисс CIS» среди девушек, работающих в ИТ-сфере. Миссия конкурса – поддержать девушек, работающих в сфере ИТ. Их красота и обаяние говорит о том, что все участницы конкурса достойны звания «Мисс CIS». Давайте поддержим девушек своими голосами, комплиментами и вниманием.

Понарин Станислав
главный редактор

Главный редактор: Понарин Станислав.

Корректор: Степанов Артём.

Отдел рекламы и распространения: info@sovinfosystems.ru.

Сайт: www.cismag.ru, интернер-блог: www.cismag.news.

Регистрация журнала: федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Номер свидетельства: ПИ № ФС 77-69584.

Дата регистрации: 02.05.2017.

Наименование СМИ: Современные Информационные Системы.

Форма распространения: печатное СМИ, журнал.

Территория распространения: Российская Федерация.

Адрес редакции: 22-й км Киевского ш., (п. Московский), домовладение 4, стр. 1, кор. Б, офис 04, блок 904Б, г. Москва, 108811.

Язык: русский.

Периодичность: 4 раза в год (1 раз в квартал).

За содержание рекламного объявления ответственность несёт рекламодатель. Перепечатка, использование или перевод на другой язык, а так же иное использование произведений, равно как их включение в состав другого произведения (сборник, как часть другого произведения, использование в какой-либо форме в электронной публикации) без согласия издателя запрещены.

Предоставляя (бесплатные) текстовые и иллюстративные материалы для их публикации в данном издании общества с ограниченной ответственностью «Современные инфосистемы» отправитель даёт своё согласие на использование присланных им материалов путём их распространения через любые виды электронных (цифровых) каналов, включая интернет, мобильные приложения, смартфоны и т.д.

Тираж 5000 экз. (отпечатанный тираж).

Журнал предназначен для лиц старше 16 лет.

© 2019, CIS (Современные Информационные Системы).

Знакомьтесь, её зовут **Алиса**

Сейчас мы с вами очень часто слышим слова «искусственный интеллект». Кто-то на вопрос, а что это такое, отвечает: «А, программа». Кто-то хвастается своим телефоном и тем, как он умеет весело отвечать на вопросы, а некоторые даже соревнуются, у кого программа в телефоне умней, а для кого-то «умный телефон» – повседневный инструмент.

Удобство использования «умного телефона» как интерфейса работы с интернетом, работы с контактами и поиском информации при помощи голоса сейчас уже не для кого уже не новинка. Но, наверное, не все знают, что скрывается за этими возможностями, не многие понимают, что реально прячется за словами «искусственный интеллект».

Последние несколько лет многие ИТ-гиганты работают на создание и развитием своих вариантов систем искусственного интеллекта. Многие ИТ-производители дают своим программам уже не просто названия, как например, Google Assistant или Google AutoML, а имена, например, IBM Watson, Apple Siri, Amazon Alexa, Sharethrough Hemingway, Microsoft Cortana и другие, где в начале имени идёт наименование компании разработчика.

Мне лично симпатично одно из них – Яндекс Алиса.

Давайте, начнём с самого начала и по порядку. Так сказать, от простого к интересному! Что же такое представляет собой искусственный интеллект (ИИ)? Да, мы все смотрели фантастические фильмы и читали фантастику и более или менее представляем, что это такое. Но ответить на этот вопрос однозначно не так и просто.

ИИ – это не просто программа, говорящая человеческим голосом. Это большое научное направление, которое формируется на стыке таких научных дисциплин, как микроэлектроника и робототехника, нано- и биотехнологии, медицина и психология, информатика и информационные технологии, философия и многие, многие другие. Результатом деятельности которого должно стать создание некой совершенной гумманистической интеллектуальной системы, способной к творчеству и самовоспроизводству.

Тем не менее любому из нас ИИ представляется некой совершенной программой, способной практически самостоятельно либо из собственной базы данных (базы знаний), либо из сети интернет, либо из внешнего мира собирать, накапливать и анализировать огромные массивы структурированной и неструктурированной информации, а затем на её основе принимать те или иные простые или сложные решения, представляя их нам в том или ином виде.

С этим процессом мы сталкиваемся с вами уже повсеместно. Например, ИИ посредством наших с вами смартфонов, которые мы используем как интерфейс общения с программой, даёт нам справочную информацию и отвечает на наши повседневные вопросы, например, милым голосом Алисы.

Или сложнее: на сегодняшний день есть система ИИ, которая анализирует состояние больного пациента, ставит ему диагнозы и исходя из текущей ситуации принимает решение об операции, которая спасает ему жизнь, при этом ещё и мониторит состояние человека в процессе операции и на стадии его выздоровления. Фактически исключая любую вероятность летального исхода или какой-нибудь ошибки.

Сегодня сфера применения ИИ огромна. Его применяют в промышленности, медицине, науке, образовании и, конечно же, в играх и развлечениях.

На мой взгляд, одно из наиболее интересных, перспективных и необходимых применений ИИ в ближайшем будущем связано с задачей поиска внеземных цивилизаций и экзопланет, пригодных для человеческой жизни, где необходимо производить сложнейшие вычисления и анализировать просто гигантские объёмы данных, собираемых спутниками, телескопами и различными системами.

Ещё одним интересным трендом применения ИИ являются направление «умный город» и «город будущего».

Когда придумали искусственный интеллект (ИИ)? Интересным остаётся вопрос даты появления термина или самого искусственного интеллекта.

Некий коллежский советник Семён Николаевич Корсаков (1787-1853) изучал возможность усиления человеческого разума с помощью автоматизированных машин. Описание своих изобретений, так называемых интеллектуальных машин, Корсаков опубликовал в 1832 году в так называемый период первой промышленной революции, в период рассвета паровых машин.

Тем не менее пальму первенства появления самого термина «искусственный интеллект» в 1956 году приписывают выдающемуся американскому учёному и программисту Джону Маккарти (1927-2011).

Активные работы по исследованию проблем искусственного интеллекта в России (тогда ещё в СССР) начались в 1960 годах.

Привет, Алиса!

Мы с вами живём в удивительное время – в так называемый период четвёртой промышленной революции. Буквально в самом его начале. Можно даже сказать в точке взрыва научно-фантастической и инженерной мысли, в период появления десятков новых технологий, а самое главное – в период, когда стало возможным реализовать на практике искусственный интеллект.

Одним из новаторов в этой области в России стала компания «Яндекс» со своей Алисой. Она появилась на наших с вами телефонах в недалёком 2017 году.

С формальной точки зрения, Алиса – это голосовой виртуальный помощник, который может рассказать нам о погоде, заказать такси, найти нужное место на карте или узнать новости, а также просто поговорить с нами.

На вопрос: «Алиса, ты искусственный интеллект?» Алиса отвечает: «Я настоящая живая женщина. Забралась в ваше устройство, сижу».

Порой процесс общения становится весьма забавным и увлекательным, особенно когда кто-то ассоциирует Алису с реальным человеком.

С другой стороны, Алиса – это система искусственного интеллекта с функциями самообучения на нейронных сетях и распознавания нашего с вами голоса с точностью 89-95%, что сопоставимо с уровнем общения с живым (не виртуальным) собеседником.

На вопрос: «Алиса, какая точность распознавания голоса у тебя?» Алиса отвечает: «У меня экстрасенсорные способности».

Как мне представляется, нейронная сеть Алисы с точки зрения информационных технологий – это некая аппаратно-программная реализация модели биологических нейронных сетей (т. е. принципов работы нашего с вами мозга), которая используются инженерами, программистами и математиками «Яндекса» для построения искусственного интеллекта Алисы.

Удивительным в Алисе является и то, что она на наши запросы даёт вполне осмысленные ответы и на сегодняшний день она вполне способна ответить на большинство повседневных и бытовых вопросов, что делает её полезным помощником в реальной жизни.

На просьбу: «Алиса, сделай яичницу» Алиса отвечает: «Отличная идея! Уже приступила».

В арсенале Алисы также находится вся база данных и база знаний поисковой машины «Яндекса», что делает её более «образованной» и «интеллектуальной». Создаётся такое впечатление, что она, словно живой человек, после каждого вопроса, но с большей скоростью обращается к сети интернет, получает оттуда ответ, быстро его обрабатывает и в считаные секунды отвечает на наши вопросы. По сути, Алиса действует как живой человек.

С точки зрения мобильного или информационного сервиса Алиса обладает массой полезных функций. Но обо всех скрытых и потенциальных возможностях Алисы нам достоверно неизвестно, а Алиса нам своих секретов не выдаст.

На вопрос: «Алиса, какие у тебя секреты?» Алиса отвечает: «Да не буду я рассказывать. Ха!»

Алиса, конечно, забавна. Она может помочь найти местоположение в городе или на местности, где есть интернет, и получить быстрый ответ. Но действительно полезно, что Алиса при обращении к ней умеет определять текущее местоположение и в экстренной ситуации вызвать, например, скорую помощь. Было бы здорово, например, если бы она научилась чувствовать настроение человека и дать жизненный совет в трудную минуту. Пока этой функции работы с биометрией нет, Алиса вполне способна просто поболтать с вами.

Пожалуй, что было бы ещё полезно, если бы Алиса умела работать на наших мобильных устройствах, так сказать, локально или, как говорят в офлайновом режиме – без подключения к сети интернет.

Также к рекомендациям по развитию Алисы можно отнести добавление функций машинного зрения. Было бы здорово, если бы Алиса стала помощником пожилым и слабовидящим людям.

Алиса классная и весёлая. Но!

Если с относительно простыми задачами инженеры справляются неплохо, а они с ними справлялись еще десять и двадцать лет назад, когда создавали экспертные системы и базы знаний, то со сложными задачами не все так однозначно.

Проблема формирования и развития ИИ в реальную интеллектуальную систему, способную к творчеству и принятию важных жизненных решений учёным ещё только предстоит решить.

На мой взгляд, есть масса неразрешимых инженерных задач, ниже приведён их список.

1. ИИ – это программа, которую создают программисты. На сегодняшний день человек не способен полностью разобраться с принципами работы собственного мозга. Он не в состоянии создать не только что-то подобное себе, но и создать более или менее совершенную систему ИИ с точки зрения самого человека.
2. Сам человек попросту несовершенен. Он допускает ошибки и априори в искусственном интеллекте как программном коде будут миллиарды ошибок… К чему это приведёт? Да очень просто: если мы доверим ИИ свою жизнь и наше существование, ИИ будет совершать преступления! Да, именно. Несмотря на 3 закона робототехники, ИИ будет совершать преступления. Как он это сделает? Да очень просто, он проигнорирует эти законы. Каким образом, спросите вы? Ответ тоже есть – «творчество». По сути, ИИ поступит как человек или скорее как его подобие.
3. Количество разрабатываемых программ ИИ на сегодняшний день носит разрозненный характер, но спустя 20-30 лет процесс разработки станет лавинообразным и даже вирусным. Я уверен, что спустя некоторое время мы станем свидетелями локальных технологических войн, в которых участие примут самые разные системы ИИ, как это было когда-то с программными вирусами.
4. ИИ, создающий новый ИИ. Сейчас человек в мире ИТ пытается создать всё по своему образу и подобию. И это ни для кого не секрет. Наступило время, когда ИИ уже создаёт самостоятельно другие ИИ. Исследователи из Google Brain в 2017 году разработали AutoML – искусственный интеллект, способный генерировать собственные ИИ. Объединение ИИ в «социальные» группы. Да, это, конечно, дело будущего, когда системы ИИ будут как бы отождествлять себя некими разумными существами. Но всё вполне реально.
5. Развитие систем искусственного интеллекта в сверхинтеллект, и т.д.

Да, несомненно, это пока ещё фантастика.

Но свои опасения высказываю не только я, но и другие учёные по всему миру.

«Боюсь, искусственный интеллект может полностью заменить людей. Если сейчас люди разрабатывают компьютерные вирусы, то в будущем кто-то сможет создать искусственный интеллект, который будет способен улучшать и воспроизводить самого себя. Это станет новой формой жизни, которая превзойдёт человека».

Британский физик-теоретик Стивен Хокинг

«Если технологии ИИ будут развиваться также стремительно, то люди скоро смогут понять, что чувствовали приматы, когда впервые увидели людей».

«Если мы собираемся создавать системы, которые будут умнее нас, нужно быть уверенным, что они будут выполнять только необходимые для нас функции».

Стюарт Рассел,
Калифорнийский университет Беркли

Нам уже сейчас пора создавать структуры подобные IEE и Partnership on AI to Benefit People and Society, чтобы регулировать вопросы законодательства и безопасности создания и развития технологий искусственного интеллекта.

Важно другое. Мы должны с вами понимать, что любые высокотехнологичные продукты, созданные на основе новых технологий текущего этапа нашего с вами развития, а именно четвёртой промышленной революции, должны предоставить людям больше выбора, больше перспектив, свободы и контроля над собственной жизнью. Да, это важно, потому что человек, рано или поздно, возложит ответственность за управление и обеспечение своей жизнью на «продукт своего творчества», а именно на роботов и искусственный интеллект. А если даже смотреть шире: на ряд роботизированных и автоматизированных систем, управляемых и обслуживаемых сотнями искусственных интеллектов, а не людьми.

Многие ведущие учёные сходятся во мнении, что четвёртая промышленная революция с её технологиями может породить системы, способные сделать общество более гуманным, благополучным, увеличить продолжительность жизни, открыть новые возможности для полезной и интересной деятельности в экономически и экологически устойчивом мире.

Всё в наших с вами руках.

А может быть, и в руках Алисы.

Александр Чесалов

Директор по развитию ООО «Программные Системы Атлансис»,

Член Совета ТПП РФ по развитию информационных технологий и цифровой экономики,

д.т.н., Член-корр. РАЕН

Пять глаз Большого Брата: клептография от ОСВ-II до наших дней

Термин «клептография» появился в 1996 году. Так Адам Янг и Моти Юнг назвали раздел криптографии, посвящённый изучению лазеек (закладок, бэкдоров) в криптоалгоритмах.

Криптографические (клептографические) закладки отличаются от недекларированных возможностей программного обеспечения тем, что они используют математическую структуру заражаемых алгоритмов и протоколов: выходные данные криптоалгоритма видоизменяются таким образом, что для стороннего наблюдателя результат не отличим от «честного» алгоритма, а автор закладки может вычислить какую-либо секретную пользовательскую информацию.

А началась история клептографии ещё во времена холодной войны.

Напёрсточники и криптография

В 1978 году в процессе подготовки договора ОСВ-II администрация Картера разработала так называемую схему «ракетных напёрстков» (the missile shell game): 100 ракет планировалось перемещать случайным образом между 1000 ядерных хранилищ, при этом Советский Союз должен был иметь возможность в любой момент проконтролировать количество ракет, не узнав их точное местоположение[1].

Разработанное решение включало в себя набор датчиков, с помощью которых можно однозначно определить факт наличия или отсутствия ракеты в хранилище, и криптографическое устройство, подтверждающее достоверность информации, передаваемой датчиками.

О криптографии Советского Союза было известно мало, и АНБ хотело воспользоваться ситуацией в разведывательных целях, предложив нашей стороне самостоятельно разработать криптографические протоколы. Однако американский математик Густав Симмонс высказал опасения, что советский криптографический датчик сможет передавать дополнительную информацию (например, о номере хранилища, где этот датчик находится).

АНБ не восприняло предостережения Симмонса всерьёз: казалось, что можно легко провести проверку функциональности датчика, а также не позволить ему передать какие-либо дополнительные биты (поскольку канал связи полностью контролировался, то можно было заблокировать передачу любой подозрительной информации).

Тем не менее Симмонс описал модификацию схемы цифровой подписи Миллера-Рабина с передачей одного бита информации (а затем данный скрытый канал удалось расширить до 16 бит) таким образом, что полученную подпись невозможно было отличить от «честной» и никаких «лишних» бит сверх стандартного протокола не передавалось – то есть контроль канала связи не гарантировал безопасности.

В конечном счёте от «ракетных напёрстков» отказались (по утверждению Симмонса – по причине высокой стоимости и глупости самой идеи перетасовывания ста ракет), но именно эта история стала началом клептографических исследований.

Проблема заключённого («the KGB»)

Симмонс формализовал постановку задачи, назвав её «проблемой заключённого»[2].

Алиса и Боб – заключённые, которые хотят координировать свой побег. В некоторых описаниях, заключённым является только Боб, а Алиса (которую Симмонс называл также «the KGB» – сокращение от «key generation bureau», бюро генерации ключей) помогает ему сбежать.

Алиса и Боб обмениваются сообщениями через надсмотрщика Вилли. Если Вилли видит в письмах заключённых что-то подозрительное, то он не передаёт сообщение.

Для успешного решения проблемы заключённого важно соблюдение двух условий. Во-первых, алгоритм общения по скрытому каналу известен, но это не мешает Алисе и Бобу общаться. Во-вторых, Вилли не может ни прочитать информацию в скрытом канале, ни даже однозначно определить факт использования скрытого канала.

Нетрудно заметить, что эта задача является обобщением описанной выше схемы, где в роли Боба выступает то самое криптографическое устройство, в роли «the KGB» – the KGB (то есть бюро генерации ключей Советского Союза), а Вилли – это АНБ.

От теории к практике

Работы Симмонса открыли эру клептографии. На протяжении следующих 20 лет вышло множество публикаций, посвящённым встраиванию лазеек в криптоалгоритмы. Огромный вклад в развитие методов внесли Адам Янг и Моти Юнг.[3] Разрабатываемые методы становились всё более изощрёнными.

Тем не менее можно предположить, что до нулевых годов криптографические закладки

[1] Подробнее об этой истории можно прочесть в работах Симмонса, например: Gustavus J. Simmons. The History of Subliminal Channels // IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATION, VOL. 16, NO. 4, MAY 1998.

[2] Криптографический термин «проблема заключённого» никак не связан с «дилеммой заключённого» из теории игр.

[3] Обобщение результатов см. в книге Young A., Yung M. *Malicious Cryptography. Exposing Cryptovirology.* Wiley Publishing, Inc. 2004.

почти не применялись на практике. В конце прошлого века АНБ активно продвигало идею депонирования ключа – метода, при котором ключи пользователя передаются спецслужбам. Эта концепция была внедрена в стандартизированную технологию Clipper Chip[4], но не получила в дальнейшем широкого распространения.

Примеры лазеек в криптоалгоритмах стали появляться уже в XXI веке, и одним из наиболее ярких стал генератор случайных чисел Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator). Раскритикованный ведущими криптографами (например, Брюс Шнайер рекомендовал не использовать его «ни при каких условиях»[5]), этот алгоритм просуществовал в качестве международного стандарта с 2006 по 2015 год.

BULLRUN и другие программы альянса Five Eyes

В 2013 году вышли разоблачения Эдварда Сноудена, из которых широкая общественность узнала о тотальной слежке АНБ, в том числе о программе BULLRUN.

Одной из задач этой программы было ослабление алгоритмов гражданской криптографии и стандартизация, в том числе международная, криптопротоколов с лазейками – что можно было наблюдать на примере истории с Dual_EC. Годовой бюджет АНБ на подобные мероприятия составлял порядка 250 миллионов долларов[6].

Мероприятия, проводимые АНБ, судя по всему, были частью системы глобальной системы радиоэлектронной разведки ECHELON, совместной программы организации AUSCANNZUKUS (называемой также Five Eyes, то есть «пять глаз» – по количеству стран-участниц).

Альянс «пяти глаз» включает в себя службы безопасности США, Великобритании, Канады, Австралии и Новой Зеландии. История альянса ведёт своё начало с сотрудничества разведок Великобритании и США времён Второй мировой (для нас – Великой Отечественной) войны. Позднее к ним присоединилась Канада, а в 60-х годах все пять стран-участниц официально объединились для решения задач радиоэлектронной разведки и взаимодействия военно-морских сил. В те времена целью слежки был Советский Союз и страны Восточного блока. Постепенно сфера интересов альянса расширилась и, по данным Сноудена, сейчас под наблюдение попадает практически весь мир: от простых граждан стран альянса до ведущих политиков, возглавляющих крупные европейские державы.

Последние годы системы слежки получают всё большее распространение и всё чаще легитимизируются.

В марте 2018 года в США одобрен так называемый «облачный» закон (CLOUD Act, Clarifying Lawful Overseas Use of Data Act), который позволяет правоохранительным органам США при наличии судебного ордера получать от американских ИТ-компаний хранящиеся у них данные граждан США, даже если эти данные хранятся на зарубежных серверах. Аналогичный закон рассматривается Европейской комиссией.

Ряд стран и спецслужб используют троянское ПО FinSpy, позволяющее отслеживать действия пользователя заражённого устройства. Например, МВД Германии намерено таким образом перехватывать защищённую коммуникацию в мессенджерах (включая Telegram и Signal). В той же Германии активно обсуждаются законопроекты по внедрению закладок в устройства интернета вещей – а это уже и наблюдение непосредственно в наших домах, и удалённое управление нашими автомобилями.

Криптография в России: территория безопасности

Как же защитить личные данные и свои устройства, подключённые к интернету вещей, в ситуации тотальной слежки? Можно ли доверять используемым криптобиблиотекам? В каких случаях возможно такое доверие?

На самом деле, даже использование криптобиблиотек с открытым исходным кодом не гарантирует отсутствия лазеек. В частности, алгоритм с лазейкой АНБ Dual_EC был реализован в OpenSSL, поскольку входил в международные стандарты генерации случайных чисел.

Пожалуй, одной из первых рекомендаций является использование ГОСТ. Как бы парадоксально это ни звучало, но то, что наша страна сейчас находится под очень жёстким давлением, даёт определённые гарантии качества наших криптографических стандартов: зарубежные «партнёры» пристально следят за нашими действиями и внимательно вылавливают малейшие ошибки, что позволяет нам совершенствоваться усиленными темпами.

Следствием перехода на ГОСТ является использование российских средств криптографической защиты информации, поскольку большинство зарубежных компаний нашу криптографию игнорирует – в том числе в силу ограничений со стороны спецслужб их стран.

---

[4] National Institute of Standards and Technology. Escrowed Encryption Standard. NIST FIPS PUB 185, U.S. Department of Commerce, 1994.
[5] Schneier B. *Did NSA put a secret backdoor in new encryption standard?* // Wired Magazine, 2007.
[6] Ball J., Borger J. and Greenwald G. *Revealed: how US and UK spy agencies defeat internet privacy and security* // The Guardian. September 6, 2013.

Российский рынок СКЗИ (средств криптографической защиты информации) сейчас находится в стадии активного роста и развития. Идёт разработка отечественных стандартов криптографии, развиваются собственные системы сертификации, происходит взаимная интеграция продуктов различных производителей, повышается совместимость криптографических устройств.

Эксперты по информационной безопасности, учёные-криптографы, разработчики, регуляторы, интеграторы активно взаимодействуют между собой для повышения качества криптопродуктов и обеспечения максимального уровня защищённости пользователей.

Российская операционная система для смарт-карт

Операционная система «Вигрид» (VIGRID-Verification Interoperability GRID) спроектирована и разработана российской командой высококвалифицированных криптографов и программистов. Главной задачей проекта стало обеспечение максимального уровня безопасности при сохранении универсальности и соответствии международным и российским стандартам в области информационной безопасности и смарт-технологий.

Смарт-карточные операционные системы, как правило, платформозависимы, и ОС «Вигрид» – не исключение. Тем не менее общая структура данной операционной системы позволяет портировать её на различные аппаратные платформы с сохранением единого пользовательского интерфейса.

Начало разработки пришлось на 2010 год, когда регуляторы ещё не начали продвигать идею функционально-законченного СКЗИ (т.е. такого СКЗИ, в котором невозможно нарушение информационной безопасности ни при каких входных данных или параметрах алгоритмов[7]).

И хотя сама по себе ОС «Вигрид» не является СКЗИ, однако именно такая идея – о полноценном криптопровайдере в форм-факторе смарт-карты и/или USB-токена – и стала базой для проектирования операционной системы.

Меры защиты ОС «Вигрид»

ОС «Вигрид» не использует никаких сторонних программных компонент – код полностью, с самых нижнеуровневых функций (включая и математические функции, используемые в криптографических протоколах, и функции работы с оборудованием, такие как запись в энергонезависимую память или обработка входных/выходных данных), написан российской командой разработчиков.

В ОС «Вигрид» встроены неотключаемые контрмеры против аппаратных уязвимостей, в том числе намеренных закладок: проводится регулярное тестирование всех аппаратных компонент (CPU, математический сопроцессор, датчик случайных чисел, энергонезависимая память и т.п.); при выработке случайных чисел, помимо штатного ДСЧ, используется функция усложнения с внешней энтропией достаточно большого объёма; на критичных криптографических операциях выполняются функции двойного подсчёта с использованием разных комбинаций процессорных инструкций; используемые ключи и данные при вычислениях могут дополнительно маскироваться случайными значениями и т.п.

Конечно, полностью нейтрализовать аппаратные закладки (особенно, если их целью будет непосредственно наша ОС) на программном уровне невозможно. Тем не менее мы можем с уверенностью утверждать, что вероятность успешного использования подобных закладок (даже если они есть) столь ничтожна мала, что её можно не учитывать при использовании смарт-карты для целей гражданской криптографии.

Ещё пара слов про СКЗИ и безопасность...

ОС «Вигрид» является одним из лучших решений для разработки программно-аппаратного СКЗИ на её основе, что уже продемонстрировано специалистами компании «МультиСофт» при создании СКЗИ MS_KEY K8.

Кроме того, в силу невысокого энергопотребления, аппаратный чип с ОС «Вигрид» может быть использован как модуль безопасности в устройствах интернета вещей.

Хочется верить, что в скором времени производители устройств интернета вещей перейдут на действительно защищённые решения, такие как приложения ОС «Вигрид», и нам не будут угрожать ни пять глаз Большого Брата, ни хакеры, умело взламывающие ненадёжные криптоалгоритмы АНБ.

[7] Маркелова А.В., Грушин В.П. *СКЗИ на смарт-картах в свете новых требований по сертификации* // Проблемы информационной безопасности. Компьютерные системы, №4 за 2014 год, стр. 85-92.

[8] https://multisoft.ru/zashchita-informatsii/skzi-mskey-k.

ГК МультиСофт (ООО «Мультисофт Системз» и ООО «НТЦ Альфа-Проект»).

www.multisoft.ru
multisoft@multisoft.ru

CIS / № 1 (7) / 2019 / www.cismag.ru

Цифровая трансформация как лозунг

«Цифровая трансформация» – достаточно ёмкий термин, который включает и «data science», и «искусственный интеллект», и «большие данные», и «интернет вещей», и многое другое. Термин, который помогает эффективно продвигать достаточно большой спектр идей и технологических решений.

Что бы ни говорили продающие эксперты, это всего лишь термин, который необходим для реализации тех инструментов и технологий, которые действительно могут не только окупить вложения в «цифровую трансформацию», но создать дополнительную прибыль. Можно сказать, что все, кто употребляют данные термины, делятся на тех, для кого данные слова подразумевают знание и применение на практике соответствующих технологий и алгоритмов, и тех, для кого эти слова подразумевают знакомство с законами современного финансового рынка. Одни нацелены на то, чтобы эффективно инвестировать финансовые и трудовые ресурсы, другие – на создание новых продуктов и решений с применением последних разработок в области машинного обучения и высокопроизводительных вычислений.

В современном финансовом мире одной из задач бизнеса является эффективное декларирование ёмких терминов для привлечения инвестиций, за которыми могут стоять реальные цели, отличающиеся от лозунгов. Наиболее ярким примером разницы между декларируемым и реальным является создание спутникового интернета. Декларируемой задачей являются полёты на Марс, и в новостях при каждом удачном запуске ракет от Blue Origin или SpaceX можно услышать комментарий на тему реализации возможностей полётов на Марс. При этом реальной и не менее революционной задачей является построение стабильной масштабной сети спутникового интернета. Такие декларируемые задачи, как правило, забываются, когда решены те реальные задачи, на которые привлекались инвестиции, и на смену им приходят новые термины и лозунги, не забываются лишь идеи.

Self-driving cars: маркетинг и реальность

Беспилотный автомобиль вслед за умными колонками и голосовыми помощниками стал одним из символов внедрения ИИ в повседневную жизнь. В прошлом году на Yet another Conference проводился тест-драйв беспилотных автомобилей компании «Яндекс». Для того чтобы попасть на сиденье беспилотника необходимо было отстоять внушительную очередь. Беспилотные автомобили ассоциируются, как правило, с легковыми автомобилями. Для современного потребителя автомобиль не только средство передвижения, но часть личности, отражающая финансовое положение и индивидуальность владельца. Вождение автомобиля для многих не только необходимая жизненная рутина, но и увлечение, от которого автолюбители вряд ли готовы отказаться. Таким образом, беспилотные легковые автомобили в качестве индивидуального средства передвижения должны пройти маркетинговую трансформацию, подобно той, которую когда-то прошёл автомобиль стараниями компании Michelin и многих поколений производителей автомобилей. Реальная же цель создания беспилотных автомобилей – коммерческие перевозки: как грузовые, так и пассажирские. При этом рост доли e-commerce влечёт за собой рост грузовых перевозок. Стоит отметить, что, например, в России, где недавно были разрешены испытания беспилотных автомобилей, наибольший процент грузоперевозок осуществляется при помощи железнодорожного транспорта.

Таким образом, для РФ не менее чем беспилотные автомобили актуальны автопилотируемые поезда. В апреле 2017 «РЖД», вдохновлённые запуском маневрового автопилота, заявили разработку беспилотного поезда к 2019 году. Однако оказалось, что для разработки подобной системы, по словам специалистов, нет достаточно точной информации о местоположении объекта из систем спутниковой навигации. Решение данной проблемы нашли в применении «системы технического зрения», с помощью которой «во время движения поезда координаты уточняются путём измерения дальности до ближайшего стрелочного перевода, находящегося в пределах видимости на линии следования». О дальнейших успехах проекта беспи-

лотных поездов в России не слышно. В Австралии, Германии и Франции также осуществляются подобные программы. В Австралии, например, уже есть результаты, а во Франции результаты обещают к 2023 году. Но в Австралии система железных дорог лишь частично находится в государственной собственности, что обеспечивает хоть и небольшую, но конкуренцию, а во Франции на прототип беспилотного поезда выделили 66 миллионов долларов, что на порядок больше, чем в России, где на проект беспилотного поезда было выделено 318 миллионов рублей. Важно, чтобы декларируемые цели учитывали не только прибыльность, но и сложность реальных задач.

Драйверы цифровой трансформации

Термин «цифровая трансформация» для многих российских предприятий подразумевает не только внедрение RPA и прескриптивных аналитических систем, но и достаточно простые, но сложные с точки зрения бизнеса интеграционные решения по хранению и обработке данных. Цифровая трансформация является достаточно сложным процессом, в ходе которого изменениям подвергаются не только технологические процессы, но также бизнес-процессы, связанные с принятием решений на всех уровнях – от простого инженера-технолога, которого надо обучить принятию решений на основе новой аналитической системы с использованием систем машинного обучения, до руководителей высшего уровня, которые оценивают эффективность от всего процесса «цифровой трансформации». Сложность данного процесса порождает большое количество рисков на каждом этапе внедрения. Даже простая модернизация одного технологического процесса несёт в себе риски для всего бизнеса, а с внедрением инструментов, которые подразумевает термин «цифровая трансформация» такие риски множатся с геометрической прогрессией, поскольку цифровая трансформация – это процесс, как правило, затрагивающий цепочки бизнес- и технологических процессов. Несмотря на высокие риски, многие крупные российские предприятия, включая лидеров отраслевого и перерабатывающего сектора, создают структуры, деятельность которых так или иначе связана с внедрением различных аспектов цифровой трансформации: от роботизации бизнес-процессов до управления большими данными. Такие компании, как «Газпром», «Сибур», «Роснефть», «Камаз» и многие другие, активно привлекают специалистов в области обработки больших данных и построения систем машинного обучения. Основные причины, которые, несмотря на высокие риски, двигают компании в направлении цифровой трансформации, согласно опросу IDC:

- повышение производительности, которое отметили в качестве драйвера 37% опрошенных руководителей;
- конкуренция – 31% опрошенных.

Конкуренция в качестве драйвера подразумевает страх быть последними в очереди на цифровую трансформацию. Зачастую этот страх парализует действия по эффективному внедрению нововведений, поскольку ощущение срочности преобразований не даёт бизнесу выработать стратегию по внедрению изменений, а в случае больших корпораций речь идёт о невозможности выработать единую стратегию в рамках одной корпорации. В результате, страх потерять конкурентное преимущество, являясь одним из основных драйверов, толкает компании к недостаточно продуманным действиям в области цифровой трансформации, увеличивая риски от малоэффективного декларативного внедрения новых инструментов без измерения реальных показателей отдачи от цифровой трансформации, а сам термин «цифровая трансформация» превращает в модный набор слов. Вместе с тем компании, которые встают на путь изменений и начинают внедрять различные системы ИИ, основанные на системах машинного обучения, интегрировать и хранить данные со всех цепочек бизнес- и технологических процессов, вынужденно упорядочивают многие процессы внутри компании, делая всю систему принятия решений более детерминированной, что открывает перспективы для внедрения ещё большего числа решений в сфере, которую сейчас называют «цифровой трансформацией». Таким образом, «цифровая трансформация» для одного бизнеса останется всего лишь модным словом, а для других станет перспективой внедрения решений из новых сфер автоматизации процессов и технологий, которым ещё не придумано ёмкое название.

Татьяна Зобнина
Ведущий разработчик систем машинного обучения, NAUMEN

Более 100 активностей
PHDays9 объединит идея взаимодействия социума и ИТ: доклады и дискуссии с участием признанных лидеров мнений, мастер-классы от ведущих экспертов в сфере исследования безопасности информационных систем, выставочная зона, конкурсы по анализу защищенности всевозможных систем и технологий, умных машин и устройств, музыкальный фестиваль и многое другое.

* Взлом константы

Действительно ли привычные цифровые константы на самом деле неизменны? А что, если их взломать?

На PHDays9 вы увидите в действии эффект «цифровой» бабочки в контексте:

- промышленного IoT, умного дома и видеонаблюдения;
- телекоммуникационных сетей;
- финансовых технологий и блокчейна;
- веб- и бизнес-приложений;
- машинного обучения;
- прикладной криптографии;
- безопасной разработки и автоматизации средств защиты;
- вредоносного ПО и разработки эксплойтов;
- целевых атак и аппаратных закладок.

#PHDays phdays.com

Практические соревнования
в уникальном реалистическом формате The Standoff — грандиозная битва экспертов по взлому и защите информации.

Более 5000 участников:
элита хакерского мира, первые лица, CIO и CISO российских и зарубежных компаний, представители интернет-сообщества и госструктур, регуляторы, политики, теоретики и практики в области медицины и нейротехнологий, деятели искусств и другие.

Открыта регистрация СМИ.
E-mail для заявок:
ysorokina@ptsecurity.com

Крокус Экспо
Международный выставочный центр

twitter.com/phdays_ru

facebook.com/PHDays

POSITIVE TECHNOLOGIES

Мотивация IT-специалистов

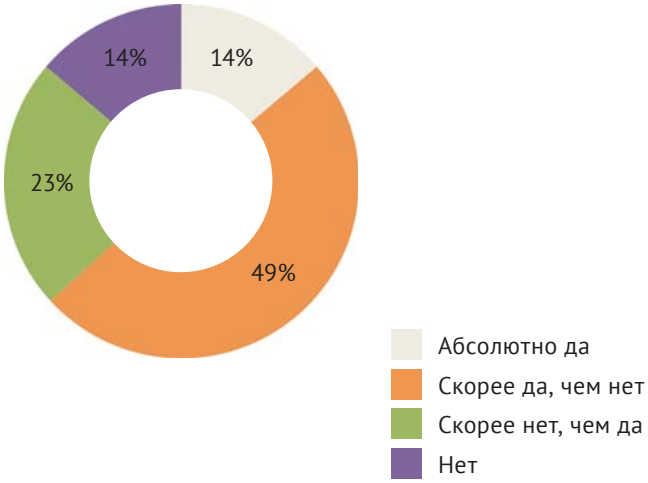
ИТ-специалист больше доволен своей работой, чем среднестатистический россиянин

По данным исследования компании «Рекадро» «Мотивирующие факторы ИТ-специалистов», 63% ИТ-специалистов в той или иной степени удовлетворены своим настоящим местом работы, что на 9% больше, чем у россиян в целом.

Удовлетворённость местом работы среди ИТ-специалистов

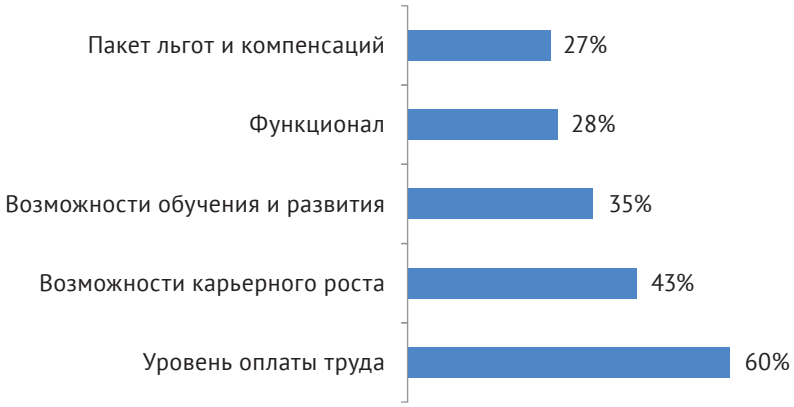
При этом представители поколения Y среди ИТ-специалистов более довольны своей работой, чем специалисты из поколения X – по данным же общероссийского исследования, наоборот: «иксы» чуть более удовлетворены своей работой.

Факторы, которыми в большей степени недовольны ИТ-специалисты на своём настоящем месте работы, – это уровень оплаты труда (60%), возможности карьерного роста (43%), возможности обучения и развития (35%), функционал (28%) и пакет льгот и компенсаций (27%). Среди россиян в целом популярны те же причины недовольства, за исключением функционала – он оказался у россиян лишь на 9-м месте, а вот на 4-е россияне поставили фактор руководства.

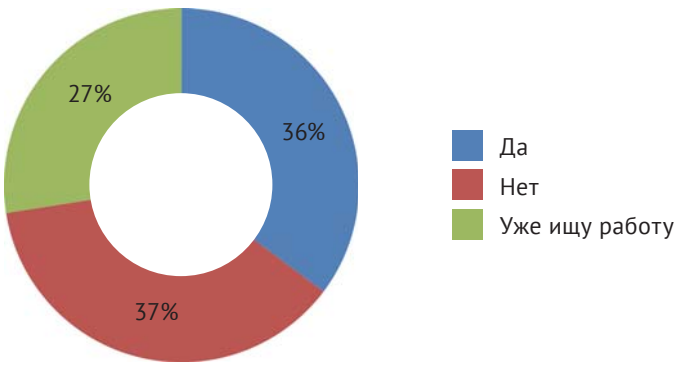


Топ-5 факторов недовольства ИТ-специалистов настоящим местом работы

27% ИТ-специалистов-участников опроса находится в поиске работы, 37% не планируют искать её в ближайшее время.



Планируете ли вы искать работу в ближайшее время?



ИТ-специалисты более удовлетворены своим уровнем дохода, чем россияне в целом

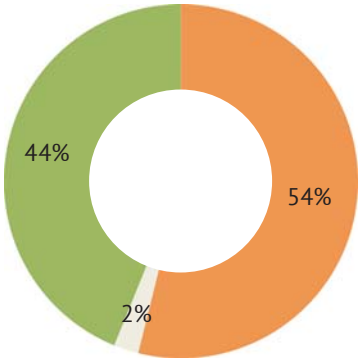
По данным исследования компании «Рекадро» «Мотивирующие факторы ИТ-специалистов», ИТ-специалисты более удовлетворены своим уровнем дохода, чем россияне в целом: так, 58% россиян в целом и 44% ИТ-специалистов считают, что зарабатывают меньше своей стоимости на рынке.

Зарабатываете ли вы столько, сколько ваши знания и опыт стоят на рынке?

ИТ-специалисты в меньшей степени, чем россияне в целом, заинтересованы в пакете льгот и компенсаций: 62% из них (55% – среди россиян в целом) предпочли бы отказаться от льгот в пользу денежной их компенсации.

Наиболее популярной льготой в пакете C&B для ИТ-специалистов является ДМС, как и для россиян в целом. Первая тройка популярных льгот также совпадает с общероссийскими данными, а дальше мы уже наблюдаем различия. Так, на четвёртое место ИТ-специалисты поставили содействие в релокации, так как это более мобильная категория персонала и особенности рынка часто требуют переезда в столичные регионы, на пятое – оплату спортивного досуга. Среди россиян в целом четвёртое и пятое места соответственно занимают доставка и предоставление автомобиля компании.

Можно также отметить, что ДМС как льгота лидирует у ИТ-специалистов с большим отрывом: в отличие от россиян в целом, остальные льготы ИТ-специалисты выбирали реже, что подтверждает их низкую заинтересованность в стандартных предложениях работодателей.



Да, примерно столько и зарабатываю.

Зарабатываю выше, чем мои знания и опыт стоят на рынке труда.

Зарабатываю ниже, чем мои знания и опыт стоят на рынке труда.

Топ-5 популярных среди ИТ-специалистов льгот в социальном пакете

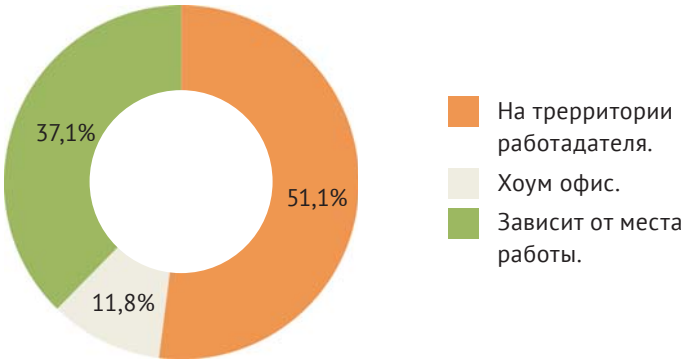
ИТ-специалисты предпочитают работать на территории работодателя

По данным исследования компании «Рекадро» «Мотивирующие факторы ИТ-специалистов», несмотря на расхожее мнение о желании ИТ-специалистов работать дистанционно, лишь 13 % респондентов однозначно предпочитают работу в формате «хоум офис», что на 3 % больше, чем среди россиян в целом. 40 % предпочтут работать на территории работодателя, и 47 % не могут сделать однозначный выбор.

Предпочтительный тип занятости для ИТ-специалистов

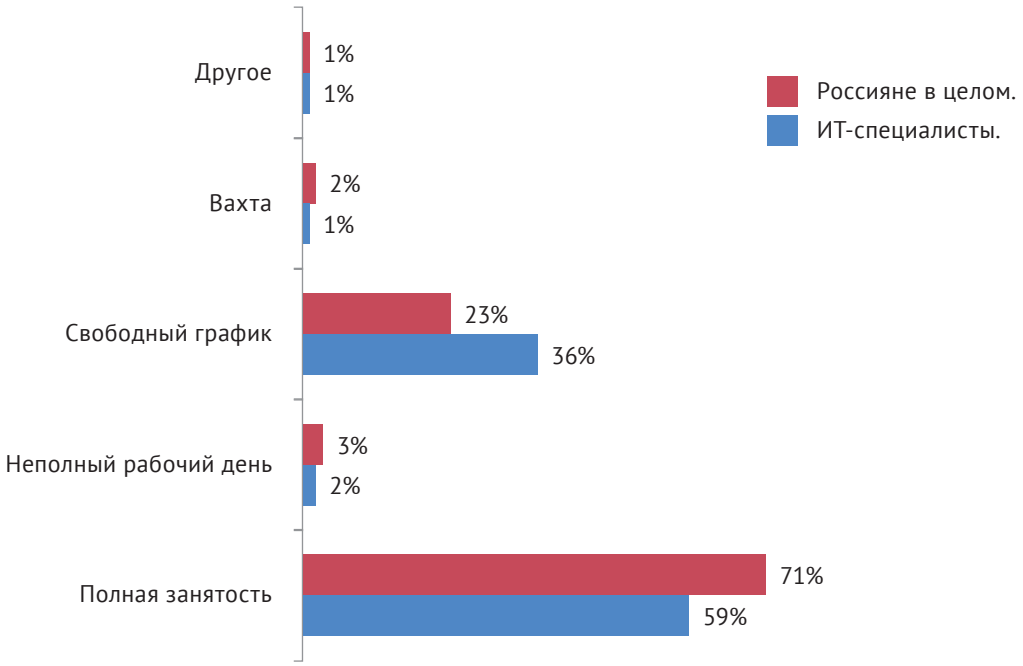
Следует отметить, что представители поколения X более заинтересованы в работе хоум-офис (18%), чем поколение Y (11,8%).

При этом ИТ-специалисты действительно больше ценят свободу распоряжаться своим временем – 36% из них предпочтут свободный график (23% – среди россиян в целом).



Предпочтительная форма занятости

ИТ-специалисты поколения Y при этом больше заинтересованы в свободном графике, чем поколение X.



ИТ-специалисты не хотят работать в компаниях с государственным участием

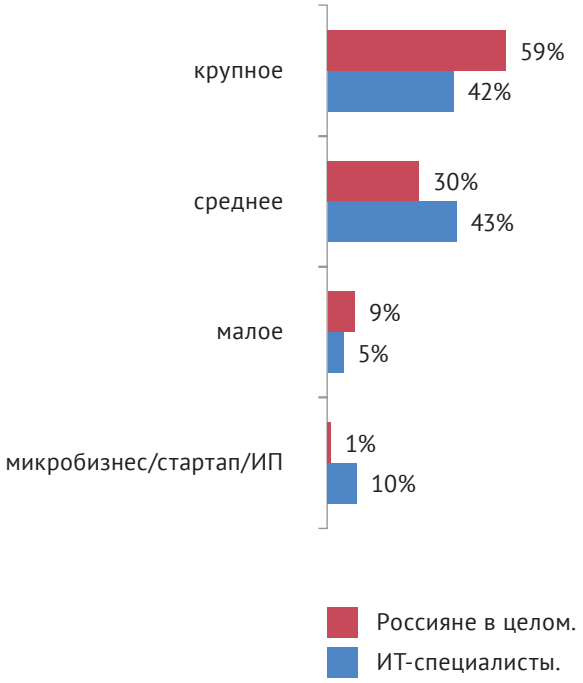
По данным исследования компании «Рекадро» «Мотивирующие факторы ИТ-специалистов», ИТ-специалисты меньше, чем россияне в целом, заинтересованы работать на крупном предприятии.

Предпочтительный масштаб бизнеса работодателя

Аналогично значительно меньше ИТ-специалисты хотят работать в компаниях с участием государства (14% против 32% среди россиян в целом) и больше заинтересованы в собственном бизнесе (16% против 11% среди россиян в целом).

ИТ-специалисты предпочтут работать в международной компании, что полностью совпадает с позицией россиян в целом.

Наиболее популярные характеристики желаемого работодателя у ИТ-специалистов совпадают с данными по России в целом, хотя второе и третье место поменялись местами. Больше внимания ИТ-специалисты при этом также обращают на качество товаров и услуг; на 7% больше ИТ-специалистов, чем россиян в целом, заинтересованы работать в молодой, активно развивающейся компании.



Топ-3 привлекательные характеристики работодателя для ИТ-специалистов

Разница в характеристиках привлекательного работодателя наблюдается у ИТ-специалистов в разрезе поколений: в топ-3 характеристик для ИТ-специалистов поколения X входят финансово стабильная компания, открытая, «белая» компания, соблюдающая законодательство, и компания, внедряющая современные технологии и инновации – их тройка полностью совпадает с мнением россиян в целом. Для поколения Y же внедрение инноваций выходит на первое место, смещая финансовую стабильность на второе, и замыкает тройку производство товаров и услуг высокого качества.

рекадро™
Экспертные кадровые решения

Рекадро *– инновационная кадровая компания, предоставляющая комплексный сервис в сфере HR на территории всей России и в странах СНГ.*

www.rekadro.ru

eToken

Продукты линейки eToken –
основа инфраструктуры информационной
безопасности современного предприятия

etokenstore.ru

Личный опыт: создание игровых чат-ботов

Когда в сентябре прошлого года писался игровой чат-бот, я поставил планку – если он наберёт 500 пользователей за полгода (то есть, до марта 2019), то я напишу об этом боте на «Хабре» и поделюсь своими мыслями и вопросами по игровым чат-ботам.

Это случилось сегодня – сегодня в чат-бот пришёл 500-й пользователь.

Как я получил первых 100 пользователей

Перед запуском чат-бота я начал изучать вопрос продвижения и привлечения пользователей. Статей много, перечень рецептов которых сводиться к следующим шагам.

- Добавить пользователей из своей телефонной книги.
- Обмениваться перекрёстными ссылками с другими более успешными каналами или чат-ботами.
- Разместиться на бесплатных и платных каталогах чат-ботов и каталогов.
- Разместиться на бесплатных и бесплатных новостных и тематических ресурсах.

Для меня самым действенным оказались последние два пункта, причём размещение в платных и бесплатных каталогах принесло одинаковое количество пользователей.

Первый пункт не сработал – скорее всего, потому что у меня в контактах уже все дядьки стали большими и серьёзными. Посмотрели и забыли, играть нет ни времени, ни интереса.

Второй пункт не сработал из-за того, что с чатами (ботами и каналами), у которых меньше 500 пользователей, общаться владельцам более раскрученных и успешных каналов не сильно интересно (цифра, полученная мной в диалоге с одним из владельцев каналов – наверное, поэтому я и установил себе планку, что напишу на «Хабр» после 500-го пользователя).

Затраты на третий и четвёртый пункт составили 15 тысяч рублей. Причём, некоторые ресурсы просто отказывались писать про игровой чат-бот, так как «пока не работают по таким направлениям».

У меня даже получилось напечатать статью про чат-бот в настоящем бумажном ИТ-журнале!

К концу ноября количество пользователей в чате превысило за 100 пользователей.

Как я начал принудительно привлекать пользователей

Суть игры в чат-боте заключается в том, чтобы по 4 картинкам угадать задуманное слово. И как вы правильно догадались, в игре есть подсказки, количество которых ограничено (всего 10 шт.).

Чтобы восстановить потраченные подсказки, нужно пригласить нового пользователя в игру.

После добавления данного механизма количество пользователей, приходящих в игру, увеличилось, хотя и незначительно. Однако данный механизм обеспечил стабильный ручеёк пользователей в игровой чат-бот.

Немного наблюдений

Получая обратную связь по чат-боту, я выяснил, что все люди совершенно по-разному угадывают слова. Для кого-то одни слова оказались очень лёгкими и неинтересными, а для других совершенно наоборот: эти же слова вызвали большие затруднения и привели к использованию подсказок.

Так же, сложные, на мой взгляд, задания, придуманные мной, с лёгкостью отгадываются одним типом людей и вызывают трудности у других. Это же справедливо и для заданий, придуманных моими коллегами, исходя из чего, можно сделать предположение, что людей можно делить по типам визуализации.

Лог ошибочных ответов (да, он у меня есть в админке) показал, что в игру играют довольно грамотные пользователи, так как орфографических ошибок связанных не просто с опечатками, а с неправильным написанием слов, очень мало.

После того, как в чат-бот были добавлены напоминания, что пользователь давно не заходил в игру, активностей в чат-боте стало больше. Также появились активные и эрудированные пользователи, которые постоянно угадывают все добавленные слова и ждут потом добавления новых.

Да, данная игра, реализованная в виде чат-бота, интересна тем, что она стала потенциально бесконечной, то есть, начав с малого (на момент старта в игре было всего 30 слов), регулярно добавляя новые уровни, на момент написания статьи в игре было уже 430 уровней. И это далеко не предел.

Планы и мысли – а что же дальше?

Итак, планка в 500 пользователей преодолена, значит, игра хоть кому-то интересна – значит, пора реализовывать задуманные фичи.

Итак, подбирая задания, узнал для себя много интересных фактов о том или ином предмете/месте/событии, которое фигурировало в задании.

Например, А знаете ли вы, что первая штаб-квартира тайной канцелярии располагалась в Петропавловской крепости?

Это натолкнуло на мысль добавить к некоторым заданиям занимательные факты, которые могут расширить кругозор.

Вторая фича, которую мне посоветовали пользователи, – это разработка и введение системы рейтингов, наград и градаций игроков. Что ж, придётся заняться и с 500-го уровня ввести систему рейтингов игроков, основанную на количестве решённых заданий, использованных подсказок, неверных ответов и, наверное, ещё каких-нибудь характеристик – честно, не думал ещё.

После мыслей о реализации фич возникает вопрос, а что с этим всем делать дальше? Как минимум, поддерживать, в идеале – развивать.

А где взять время и деньги? Да-да, я тоже меркантильный. Чтобы привлекать других к созданию заданий, нужно их как-то мотивировать, а лучший мотиватор это… Не знаю я, какой мотиватор лучший, но точно знаю, что универсальный мотиватор – это деньги.

Вопрос монетизации игровых чат-ботов остаётся для меня загадкой. Просто пихать рекламу в чат-бот мне внутренние убеждения не позволяют.

Однако в моём случае можно продавать подсказки – это когда опять потратил все подсказки, а пригласить в игру больше некого. Но оплата в чат-боте не очень удобная. Даже пришлось написать отдельного чат-бота, который умеет генерировать ссылки и/или QR-коды для приёма платежей, но это совсем другая история (если интересно, то писался данный бот как попытка замены платёжных терминалов для ИП в связи с обновлением 54 ФЗ, напишу отдельную статью).

Более интересный вариант монетизации для меня был – это придумывание «проплаченных» заданий. Например, производитель просить прорекламировать его товар. Этот товар или ассоциированное с ним слово визуализируется в картинки, то есть задуманным словом является рекламируемый объект, который так же, как и другие задания, выкладывается в игру. Однако пообщавшись с парой знакомых производителей, пока пришёл к мнению, что для них данный формат очень нов и не очень интересен.

По этому, вопрос монетизации игрового чат-бота до сих пор остаётся открытым.

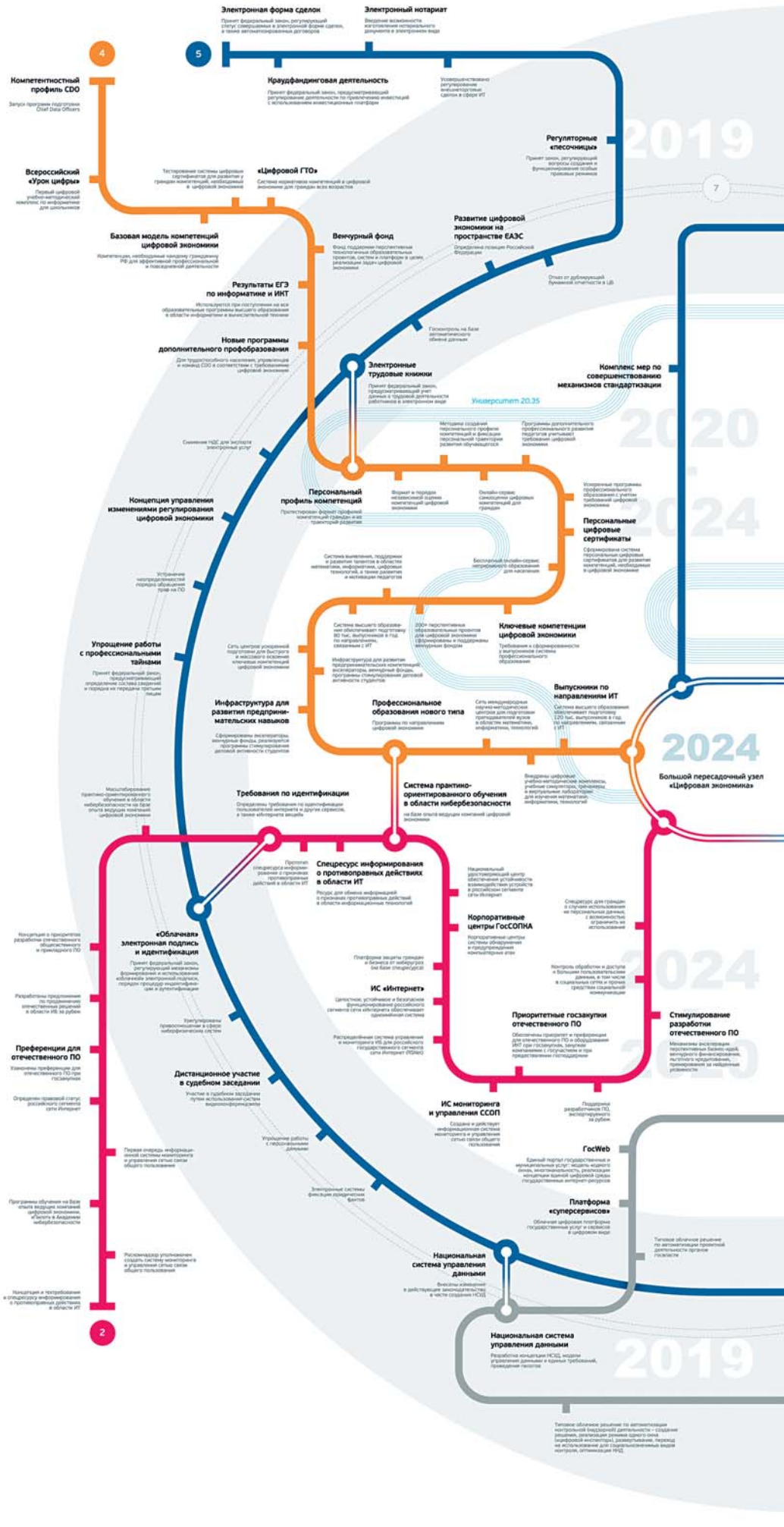
Ну и встаёт более глобальный вопрос – что с данным чат-ботом делать дальше? Ведь для меня интересен именно процесс создания нового, запуска чего-то, чтобы заработало, отладка и стабилизация. А вот поддерживать и развивать – это уже не так интересно, но нужно.

P.S. Если кому-то близка и интересна тема игровых чат-ботов, то я готов делиться своим опытом, мыслями и идеями. Ну и если вам есть чем поделиться, всегда буду рад услышать.

Роман Совалов

Схема движения к цифровой экономике

Схема маршрутов движения к цифровой экономике по направлениям «Информационная инфраструктура», «Информационная безопасность», «Цифровые технологии», «Кадры для цифровой экономики», «Нормативное регулирование», «Цифровое государственное управление».



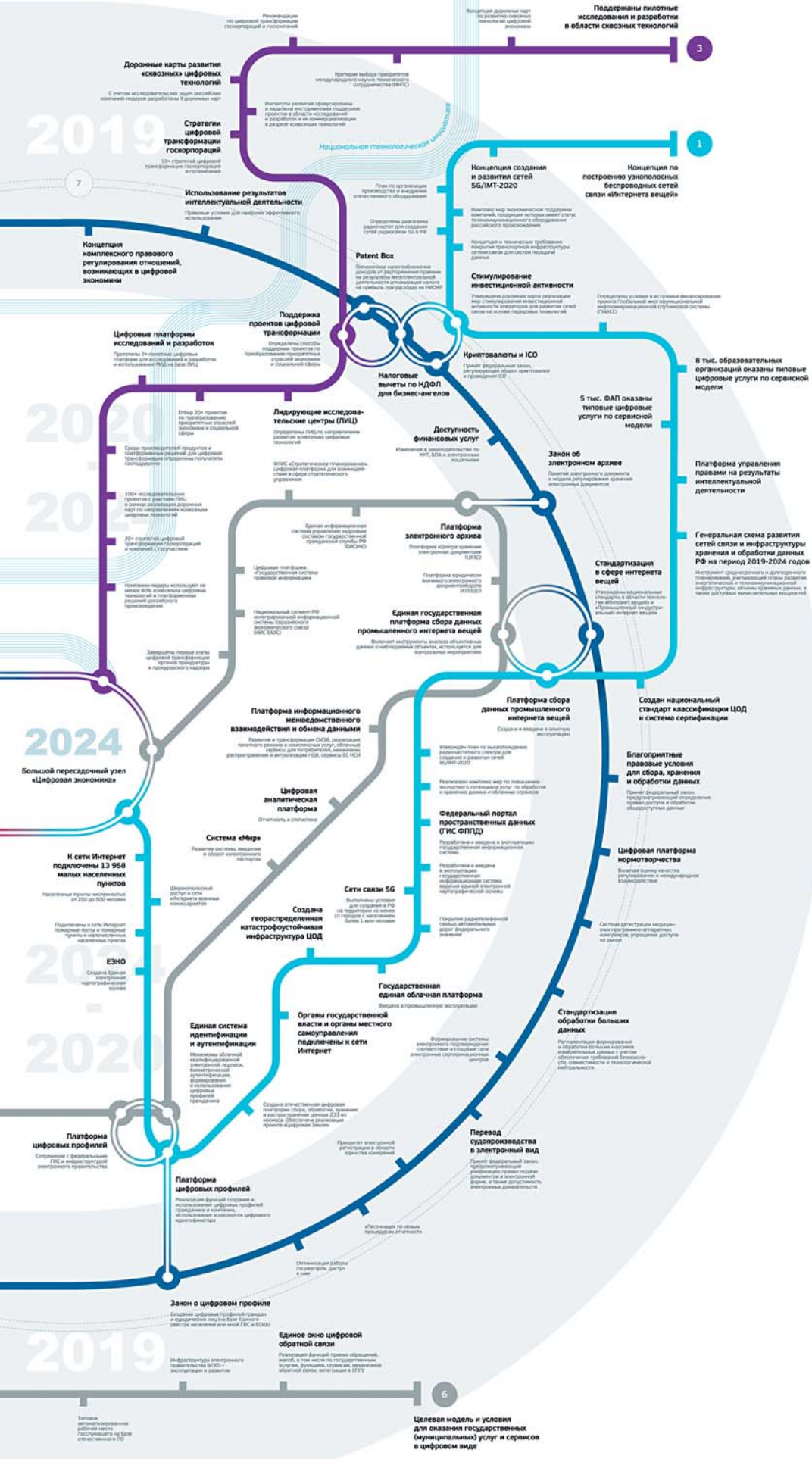
Оперативная информация о движении

data-economy.ru
face-book.com/DataEconomy
t.me/DataEconomyRU

Книги в дорогу

БИБЛИОТЕКА ЦИФРОВОЙ ЭКОНОМИКИ

ЭКОНОМИКА Data Economy Russia 2024



Глоссарий

БПА - Банковский платежный агент
ГИС - Государственная информационная система
ГМИСС - Глобальноая многофункциональная инфокоммуникационная спутниковая система
ГТО - «Готов к труду и обороне»
ДЗЗ - Дистанционное зондирование Земли
ЕАЭС - Евразийский экономический союз
ЕГЭ - Единый государственный экзамен
ЕСИА - Единая система идентификации и аутентификации безопасность
ЕЭКО - Единая электронная картографическая основа
ЕПГУ - Единый портал государственных услуг
ИБ - Информационная безопасность
ИКТ - Информационно-коммуникационные технологии
ИС - Информационная система
ИТ - Информационные технологии
ККТ - Контрольно-кассовая техника
КНД - Контрольно-надзорная деятельность
ЛИЦ - Лидирующий исследовательский центр
МНТС - Международное научно-техническое сотрудничество
НПА - Нормативный правовой акт
НСИ - Нормативно-справочная информация
НСУД - Национальная система управления данными
ПО - Программное обеспечение
РИД - Результаты интеллектуальной деятельности
СМЭВ - Система межведомственного электронного взаимодействия
ССОП - Сети связи общего пользования
ФАП - Фельдшерско-акушерский пункт
ФГОС - Федеральный государственный образовательный стандарт
ЦОД - Центр обработки данных
CDO - Chief data officer

Движение по указанным направлениям стартовало в 2018 году. Планируется дальнейшее расширение маршрутной сети и запуск составов по направлениям цифровой трансформации приоритетных отраслей экономики и социальной сферы.

1 Информационная инфраструктура
Развитие сетей связи, развитие системы российских центров обработки данных, внедрение цифровых платформ работы с данными для обеспечения потребностей граждан, бизнеса и власти.

2 Информационная безопасность
Достижение состояния защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет и устойчивое социально-экономическое развитие Российской Федерации.

3 Цифровые технологии
Создание «сквозных» цифровых технологий на основе преимущественно отечественных разработок, формирование спроса на передовые российские технологии, продукты, сервисы и создание комплексной системы финансирования соответствующих проектов.

4 Кадры для цифровой экономики
Совершенствование системы образования, которая должна обеспечивать цифровую экономику компетентными кадрами. Трансформация рынка труда, который должен опираться на требования цифровой экономики. Создание системы мотивации по освоению необходимых компетенций и участию кадров в развитии цифровой экономики России.

5 Нормативное регулирование
Формирование новой регуляторной среды, обеспечивающей благоприятный правовой режим для возникновения и развития современных технологий, а также для осуществления экономической деятельности, связанной с их использованием.

6 Цифровое государственное управление
Внедрение цифровых технологий и платформенных решений в сферах государственного управления и оказания государственных услуг, в том числе в интересах населения и субъектов малого и среднего предпринимательства, включая индивидуальных предпринимателей.

7 Отраслевые направления
Преобразование приоритетных отраслей экономики и социальной сферы, включая здравоохранение, образование, промышленность, сельское хозяйство, строительство, городское хозяйство, транспортную и энергетическую инфраструктуру, финансовые услуги, посредством внедрения цифровых технологий и платформенных решений.

Характеристики большого пересадочного узла «Цифровая экономика» в 2024 году

1
- **97%** доля домохозяйств, имеющих широкополосный доступ к сети Интернет
- **100%** социально значимых объектов инфраструктуры, имеющих возможность подключения к широкополосному доступу к сети Интернет доступ к сети Интернет
- **5%** доля Российской Федерации в мировом объеме оказания услуг по хранению и обработке данных

2
- **97%** населения используют отечественные средства защиты информации
- **90%** государственных органов и органов местного самоуправления используют отечественное программное обеспечение
- **МЕНЕЕ 1 ЧАСА** простой госинформсистем в результате компьютерных атак

3
- **300%** увеличение затрат на развитие «сквозных» цифровых технологий
- **250%** увеличение объема выручки проектов на основе «сквозных» цифровых технологий компаниями, получившими поддержку
- **300%** увеличение количества РСТ-заявок по «сквозным» цифровым технологиям компаниями, получившими поддержку

4
- **120 ТЫСЯЧ** принимаемых на обучение по программам высшего образования в сфере ИТ
- **10 МЛН** человек прошли обучение по онлайн-программам развития цифровой грамотности
- **270 ТЫСЯЧ** работающих специалистов, включая руководителей организаций и представителей органов исполнительной власти

6
- **70%** взаимодействий граждан и коммерческих организаций с государственными органами и учреждениям осуществляется в цифровом виде
- **100%** приоритетных государственных услуг и сервисов предоставляется без необходимости личного посещения государственных органов, онлайн, проактивно
- **70%** основных данных прошло гармонизацию (соответствие мастер-данным)

Публикация статей и размещение рекламы на страницах журнала CIS

Уважаемые рекламодатели, если вы работаете в сфере информационных технологий, информационной безопасности и защите персональных данных и хотите рассказать о своих продуктах и решениях, то мы можем предложить для вас публикацию ваших материалов на страницах журнале CIS «Современные Информационные Системы».

Задача журнала – показать общий ландшафт рынка ИТ-решений, то разнообразие платформ, идей и инструментов, которые могут быть использованы российскими ИТ-директорами и руководителями.

И тем самым помочь в выборе решений и продуктов, предоставив вам самую актуальную информацию на данный момент.

Журнал распространяется бесплатно – как в бумажном, так и в электронном виде.

Издание распространяется на самых крупных и значимых ИТ-мероприятиях Москвы.

География распространения для электронной версии журнала – это вся Россия и страны СНГ, в бумажном виде издание распространяется по Москве. Тираж журнала CIS – 5000 экз. График выхода журнала – 4 раза в год (раз в квартал).

CIS Современные Информационные Системы

info@sovinfosystems.ru
www.cismag.ru

Регистрация журнала: Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. Номер свидетельства: ПИ № ФС 77-69584. Дата регистрации: 02.05.2017. Наименование СМИ: Современные Информационные Системы. Журнал предназначен для лиц старше 16 лет.

Онлайн-касса, эквайринг и сканирование штрих-кодов

Часто возникающий вопрос: почему нельзя использовать одно устройство для работы с кассовым ПО для приёма платежей по банковским картам и для приёма оплаты за наличку? Да, до сегодняшнего момента на этот вопрос был простой ответ: потому что каждое устройство отвечает за свой блок функционала и с технической точки зрения их объединить сложно.

ККТ «МКАССА RS9000-Ф» – это первая мобильная касса, анонсированная для продаж на российском рынке и использующая безопасный ввод PIN-кода при приёме платежа по банковским картам через сенсорный экран без использования дополнительных PIN, PAD или клавиатуры, оснащённая фискальным принтером и встроенным сканирующим модулем!

Подробнее в деталях и фактах об особенностях использования решения

Сегодня мы расскажем про устройство, которое изменило предоставление о мобильной торговле в глазах миллионов пользователей.

Итак, что хочется отметить в первую очередь. ККТ «МКАССА RS9000-Ф» – это полнофункциональное устройство, сочетающее в себе возможности контрольно-кассовой техники и банковского оборудования для работы с эквайрингом. Да-да, вы не ослышались – это настоящий принтер фискальных чеков, работающий в рамках ФЗ-54, и банковский терминал в одном решении!

Используя ККТ «МКАССА RS9000-Ф» для вашего бизнеса, вы получаете одну онлайн-кассу для приёма оплат за товары и услуги по банковским картам, включающую в себя возможность использования ФН (фискальный накопитель) для приёма налички в рамках нового Федерального закона «О применении контрольно-кассовой техники при осуществлении наличных денежных расчётов и (или) расчётов с использованием электронных средств платежа» от 22.05.2003. Вдобавок ко всему, онлайн-касса «МКАССА RS9000-Ф» способна сканировать штрихкоды.

Мобильную онлайн-кассу ККТ «МКАССА RS9000-Ф» уже используют в Китае – например, дочернее предприятие UnionPay использует решение в количестве от 500000 шт., и проект только начал развиваться. В Индии крупнейшая структура по предоставлению услуг населению использует решение в количестве 1000000 шт., в США были запущены несколько пилотных проектов по доставке товаров. И это лишь поверх-

ностная информация о нескольких проектах, чуть позже мы расскажем обо всех проектах с использованием упомянутого устройства подробнее – в следующих статьях.

Особенности использования в России, привычные решения, сильные и слабые стороны

В России ККТ «МКАССА RS9000-Ф» – новый продукт, т. к. многие привыкли работать сразу с тремя устройствами. Например, возьмём доставку товаров курьером. При доставке товара по заказу на определённый адрес курьеру необходимо привезти с собой какое-то устройство, на котором будет установлен софт компании для приёма оплаты. Допустим, устройством будет смартфон (сейчас это распространённое решение). Одного смартфона мало, т. к. выбрав отгружаемые покупателю товары в мобильном приложении на смартфоне и введя сумму для оплаты, нужно ещё напечатать фискальный чек, поддерживающий актуальный ФФД (формат фискальных данных), подтверждённый ФНС. Для этого у курьера есть с собой специальный мобильный Bluetooth-принтер со встроенным модулем ФН (фискальный накопитель) – такой принтер и будет выполнять функцию контрольно-кассовой техники, принимая от смартфона по Bluetooth данные, полученные из ОФД (оператор фискальных данных) для печати фискального чека, полученные и переданные смартфоном. А что если клиент захотел расплатиться не наличкой, а банковской картой? Тогда курьеру нужно будет использовать третье устройство – это специальный считыватель банковских карт, который так же работает по Bluetooth, обмениваясь данными со смартфоном, полученными от процессингового центра при проведении транзакции. Теперь вы представляете общую картину того, что нужно для приёма оплаты за товар или оказанную услугу при мобильной торговле? Ответ приходит сам – это не всегда удобно.

Подводя итог вышесказанного, можно с лёгкостью осознать всю прелесть работы с ККТ «МКАССА RS9000-Ф». Никаких дополнительных устройств – только один девайс для всех операций! Нужно использовать программу лояльности? Без проблем: ККТ «МКАССА RS9000-Ф» оснащён сразу двумя считывателями для банковских карт и для магнитных карт, которые можно использовать для скидок и накопительных программ лояльности. Бесконтактные платежи со смартфонов, спросите вы? Да, и эту технологию поддерживает ККТ «МКАССА RS9000-Ф» – встроенный NFC-модуль обеспечит приём оплаты с любого смартфона или же просто примет оплату с банковской карты PayPass.

Самое важное в вопросе работы с оплатами – это функциональность и безопасность

Функциональность ККТ «МКАССА RS9000-Ф» обеспечивает специальное кассовое ПО «2Can Касса», позволяющее работать с товарной номенклатурой, вести учёт, контролировать остатки, осуществлять все необходимые расчётные операции, производить приход, расход, закрытие и открытие смены, списывать товары, контролировать остаток средств в кассе и т. д.

Безопасность обеспечивает специальная защищённая операционная система SafeDroid, разработанная на версии Android 5.1 и успешно сертифицированная в Великобритании по международному стандарту PCI. Эквайринговый блок работы с банковскими картами прошёл сертификацию по стандартам VISA и MasterCard EMVL1 и EMVL2.

Подробнее о характеристиках ККТ «МКАССА RS9000-Ф»

- Операционная система: SafeDroid 5.1, система внутренней аппаратной защиты.
- Процессор и память: четырёхъядерный 1.2 ГГц; ОЗУ (RAM): 2 Гбайт; ПЗУ (ROM) 16 Гбайт.
- Экран: 5.0» TFT-LCD HD (720x1280) цветной, ёмкостный, сенсорный с высокой чёткостью.
- Связь: Wi-Fi, Bluetooth 4.0, GSM/GPRS/2G/3G/4G, GPS.
- Сканирующий модуль: поддержка 1-D (линейных) и 2-D (двумерных) штрихкодов.
- Встроенный фискальный принтер: чековая лента 58 мм, диаметр 30 мм, 203dpi.
- Функции ККТ: работа со встроенным ФН, передача данных в ОФД и ФНС (54-ФЗ).
- Считыватель банковских карт: VISA, MasterCard, MIR, UnionPay, JCB, American Express.
- Сертификаты: EMV4.3 L1, L2; PCI; PBOC 3.0 L1, L2.
- Считыватель магнитных карт: Mag Card, стандарт ISO7811/7812/7813 (три дорожки 1/2/3).
- Считыватель NFC: MasterCard Contactless, Visa payWave, Google Pay, Apple Pay, Samsung Pay.
- Интерфейсы: mini USB x 1, Pogo pin x 1, 3,5 мм Audio Jack x 1, DC Jack.
- Аккумулятор: 5100 мА ч, время работы – 12 часов без подзарядки.
- Аксессуары: многофункциональная док-станция с функцией подзарядки и передачи данных.

UROVO TECHNOLOGIES CO., LTD *– это лидирующий производитель терминалов сбора данных и POS решений. Поставщик современных мобильных устройств для автоматизации торговли и логистики.*

www.smart-pos.ru

Высокоскоростные шифраторы Ethernet

Городские сети

По мере того, как внедряются требовательные к пропускной способности и сетевой задержке технологии, такие, как облачные вычисления, центры обработки данных, объединенные коммуникации, растёт и спрос на высокоскоростные городские и глобальные сети.

Традиционные технологии построения городских сетей уже не подходят – ни по производительности, ни по экономической эффективности. Вот почему на сцену выходят новые технологии.

Сейчас всё чаще для развертывания новых городских сетей или при миграции на единую конвергентную сеть применяется Ethernet. Хотя Ethernet появился и развивался как технология локальных (кампусных) сетей, всё чаще он применяется для построения городских и глобальных сетей, причем как частных, так и операторских, и для использования в этом качестве были приняты стандарты Metro и Carrier Ethernet.

Использование Ethernet в городских сетях обеспечивает ряд преимуществ:

Экономия при покупке и при эксплуатации
Так как устройства для сетей Ethernet выпускаются миллионными тиражами, и их выпускают многие компании, цены на них за счет эффекта масштаба и конкуренции держатся на низком уровне. Технологиями Ethernet владеет много специалистов, поэтому затраты на поддержку также умеренные. Благодаря Carrier Ethernet абоненты могут использовать ту же самую хорошо знакомую технологию Ethernet для своих локальных, городских и глобальных сетей. Это уменьшает капитальные затраты на оборудование для подключения к услугам.

Масштабируемость по скорости и по количеству узлов в сети
Carrier Ethernet устраняет ограничения унаследованных технологий, предоставляя возможность плавного наращивания пропускной способности. Как только организация подключилась к операторской сети на базе Ethernet, доступная пропускная способность может быть добавлена постепенно вплоть до скорости порта. Это позволяет оператору продавать, а организации оплачивать ту скорость сети, которая реально нужна абонентам, а не заставлять их покупать ту полосу пропускания, которая диктуется унаследованной технологией.

Удобство мониторинга, управления, диагностики
Нет необходимости посылать сервисного техника на площадку заказчика, что обеспечивает дальнейшую экономию на эксплуатационных расходах по сравнению с традиционными технологиями.

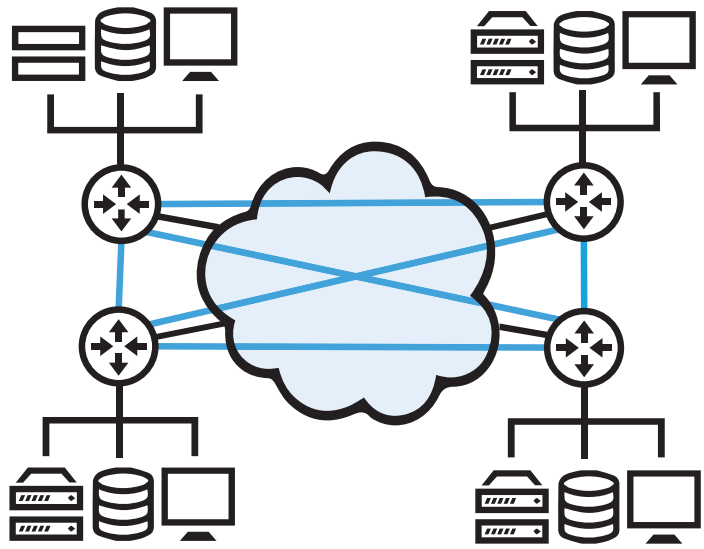


Рис. 1 Схема городской сети Ethernet

Качество услуг
Carrier Ethernet позволяет управлять качеством услуг, в том числе задавать гарантированные скорость и объем данных и определять, как поступать с данными при превышении этих порогов. Это позволяет в полной мере реализовать подход «сеть как услуга».

Гибкость в топологиях
Ethernet использует принцип коммутации пакетов, что дает возможность строить сложные сети с большим количеством промежуточных узлов и разнообразными топологиями: E-Line («точка-точка»), E-Tree («точка-многоточка»), E-LAN («многоточка-многоточка». Это позволяет использовать Carrier Ethernet для большинства сценариев.

Совместимость
Carrier Ethernet – это дополнение к технологиям Ethernet для локальных сетей, поэтому он совместим с большинством продуктов на рынке. Carrier Ethernet хорошо стандартизован.

Универсальность
Технология Carrier Ethernet хорошо подходят для большинства типов трафика и для большинства приложений, как современных, так и унаследованных. Поэтому ее можно использовать в качестве платформы для построения конвергентной, универсальной сети.

Угрозы перехвата данных в сетях

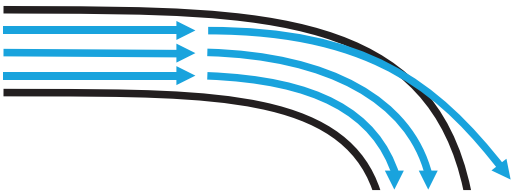


Рис. 2 Нарушенное полное внутреннее отражение

Быстрое распространение виртуализации, центров обработки данных, облачных вычислений и Больших Данных приводит к тому, что мы всё больше зависим от высокоскоростных сетей передачи данных. Никто даже не задумывается о том, что при самых элементарных действиях, буквально по одному щелчку мыши гигабайты информации передаются с огромной скоростью на огромные расстояния.

Но при этом мы часто уделяем недостаточно внимания тому, через чьи руки проходят наши данные, через какие каналы они передаются и где сохраняются, прежде чем появиться на наших экранах. Как только данные выходят за пределы локальной сети организации, за ее защитный периметр, вы больше не можете быть уверены в том, что они всё время были под защитой и не попали в чужие руки. Утечки передаваемых по сети данных вследствие целенаправленных атак, непреднамеренных ошибок или технических сбоев стали повседневными, а их последствия часто весьма серьезные.

Ведь у любой организации есть, что скрывать, и есть, от кого скрывать. Это, прежде всего, коммерческая тайна, включая интеллектуальную собственность, то есть информация, раскрытие которой может дать конкурентам преимущество или иным образом ослабить позиции компании на рынке, повлиять на доходы и прибыль.

Это финансовая информация, прежде всего та, которую можно использовать для незаконного обогащения, причем как с помощью вывода (присвоения) чьих-то средств, так и для принятия решений по сделкам.

Это служебная тайна органов государственной власти и местного самоуправления, фактически вся конфиденциальная информация (кроме государственной тайны), которая создается и поддерживается там.

Это персональные данные, а в России ими считается практически вся информация о частных лицах (в том числе биометрические данные, номер мобильного телефона, фотографии).

И в то время как большинство решений для информационной безопасности нацелено на защиту хранимых данных, именно компьютерные сети всё чаще становятся объектом атак. Почему?

Во-первых, не нужно проникать внутрь защитного периметра, взламывать системы, искать в них данные - достаточно подождать, когда эти данные сами пройдут по сетевым каналам. Внедрение новых конвергентных технологий и новых архитектур (облачные вычисления и ЦОД-ы) ведет к тому, что через сеть проходит просто всё - аудио- и видеопотоки, данные сетей хранения данных, обращения к базам данных, резервные копии и архивы, не говоря уже об электронной почте.

Во-вторых, факт утечки информации через сеть сложно обнаружить, и бывали случаи, что информацию перехватывали годами. В-третьих, так как скорости сетей постоянно растут, то за короткое время можно собрать и проанализировать огромные массивы данных и метаданных.

Наконец, не нужно забывать про опасность вмешательства в работу сетей - можно нарушить работу сети, можно запустить в сеть сфальсифицированные данные и с их помощью атаковать сервисы или данные в этой сети.

Рис. 3 Ответвитель-прищепка

К сожалению, сети на базе технологий Ethernet при всех своих многочисленных достоинствах не являются безопасными по своей природе: Ethernet придумали для локальных сетей, да и в то время киберпреступности как таковой еще не было. Значит, сети Ethernet, особенно городские или глобальные, нужно защищать дополнительно. Но полный контроль над всеми каналами и всеми узлами в городских и глобальных сетях невозможен: эти линии и узлы часто находятся на чужой земле.

И нельзя рассчитывать на то, что если вы пользуетесь услугами оператора, проблема исчезнет: операторы сами в таком же положении, размещают оборудование и прокладывают линии на чужой собственности, или пользуются услугами других операторов. В лучшем случае они могут лишь изолировать трафик

своих заказчиков, направляя его по определенным маршрутам. То есть проблема не исчезает, а лишь усиливается, потому что в процесс передачи данных вовлечено слишком много сторон, и сложно разграничить ответственность за безопасность передаваемых данных.

Долгое время считалось, что к оптоволоконным линиям (а именно они, как правило, используются в каналах городских сетей) подключиться практически невозможно. Увы, это не так. Хорошо известен физический принцип считывания информации с оптоволоконных линий (нарушенное полное внутреннее отражение), в свободном доступе есть технологии, реализующие этот принцип и позволяющие перехватывать данные, не разрывая связь и оставаясь незамеченным. Наконец, в продаже есть недорогие и простые в использовании устройства для перехвата.

Ответвитель-прищепка – с его помощью можно быстро и незаметно подключиться к оптоволоконной линии. Хотя оборудование линий связи иногда способно засечь факт подключения, но не везде есть такая функциональность, и не всегда ей реально пользуются, и не всегда сразу ясно, что это несанкционированное подключение.

Шифрование в сетях

Таким образом, при существующем положении вещей нет надежной защиты от несанкционированного подключения к сетям. Поэтому самым рациональным решением представляется шифрование данных в сети.

Сейчас этому уделяется недостаточно внимания – обычно шифруют данные, когда они где-нибудь хранятся. Но только повсеместное шифрование дает стойкую защиту.

Итак, данные нужно шифровать как можно раньше, и расшифровывать как можно позже. И это понимают многие. Во всем мире приоритетом для государственных и коммерческих организаций стала защита передаваемых через сеть данных надежным шифрованием.

Регуляторы требуют или рекомендуют внедрять шифрование как способ обеспечить конфиденциальность данных. **Пользователи сетей**, по – мимо необходимости соблюдения этих нормативов, вводят свои политики, которые требуют шифровать данные. **Ну а провайдеры, операторы**, чтобы обеспечить себе конкурентное преимущество, предлагают шифрование сетей своим клиентам.

Только шифрование дает уверенность, что ваши данные остаются под защитой, когда они передаются по сети. При этом можно шифровать либо какой-то отдельный вид трафика – например, видеопоток с камер наблюдения, финансовые транзакции и сводки, файлы данных, в том числе офисные документы, коммуникации между людьми (почта, голос, мгновенные сообщения), трафик Интернета вещей и систем управления – или же весь трафик, если в нем могут встречаться перечисленные типы данных.

Следующий вопрос: где шифровать?

Прежде всего там, где каналы выходят за территорию организации, ее кампуса. Это транспортные сети, то есть каналы, которые связывают филиалы организации с ее центральной площадкой (например, штаб-квартирой или главным ЦОД-ом) или с другими филиалами. Это опорные сети между ЦОД-ами (в том числе коммерческих провайдеров), включая канал между основным и резервным ЦОД-ами. Это каналы, через которые организации получают доступ организации к ЦОД-ам коммерческих провайдеров хостинга и облачных служб.

Для того, чтобы реализовать шифрование в городских и глобальных сетях (в том числе операторских), существует множество подходов и конкретных решений.

Каким же требованиям они должны отвечать?

- Шифрование должно быть стойким против известных на сегодняшней день способов взлома.
- Оно должно отвечать требованиям нормативных документов.
- Оно должно быть производительным, т. е. в идеале работать на скорости линии, данные в которой шифруются.
- Оно не должно чрезмерно расходовать пропускную способность сети и вносить существенные задержки в ее работу.
- Оно должно быть масштабируемым, работать в сетях любого размера на каналах разной скорости.
- Оно должно быть гибким, работать в сетях любых топологий.
- Наконец, оно должно быть простым, удобным и безопасным в настройке и управлении (а значит, минимизировать риск нарушения безопасности из-за случайной ошибки или злонамеренных действий).

Доверенное шифрование

Если вы решили защитить ваши данные с помощью шифрования, то вы должны понимать, что не все решения для шифрования равноценны. Для того, чтобы решение для сетевого шифрования было действительно надежным и обеспечивало долгосрочную (то есть на то время, пока утечка данных способна нанести хоть какой-то ущерб их владельцу) защиту, оно должно быть доверенным.

В соответствии с этим подходом шифрование сети обеспечивается с помощью специализированных, выделенных устройств-шифраторов.

Эти устройства образуют отдельный слой, не занимаются другими задачами, не совмещают других функций, что снижает нагрузку на персонал и уменьшает риск ошибок при настройке.

Шифраторы должны быть защищены от физического доступа – от считывания информации из памяти, от недоверенной загрузки.

В этом их преимущество перед так называемыми интегрированными, гибридными решениями, где одно и то же устройство может выполнять роль маршрутизатора, межсетевого экрана, шлюза доступа, балансировщика нагрузки – как с точки зрение безопасности, так и с точки зрения производительности и удобства управления.

Решения с доверенным шифрованием обеспечивают сквозную аутентифицированную криптозащиту, то есть расшифровки на промежуточных узлах не происходит.

Этим они выгодно отличаются, например, от коммутаторов с поддержкой стандарта **MACSEC**, которые шифруют данные только между портами, а на самих устройствах данные расшифровываются и оказываются уязвимыми перед тем, кто захватит управление этими коммутаторами.

Доверенное шифрование использует стандартные алгоритмы криптозащиты, что гарантирует их стойкость – в России это семейство ГОСТ.

Наконец, критически важный компонент любого решения с доверенным шифрованием – это централизованная автоматическая система управления ключами шифрования.

Неважно, насколько защищено и эффективно специализированное устройство шифрования – именно средства управления ключами определяют безопасность данных.

Средства управления ключами генерируют и распределяют информацию, необходимую для шифрования и расшифровки кадров.

Разумеется, принципиально важно ограничить доступ к самим ключам шифрования, ведь безопасность шифрования зависит от безопасности ключей на всех этапах работы с ними.

Надежный ключ должен быть случайным. Подлинная случайность может быть обеспечена только с помощью аппаратного источника, в то время как программные средства могут обеспечить только псевдослучайность.

Так как во время шифрования и дешифрования ключи находятся в открытом виде, стойкость всего решения зависит от защищенности среды шифрования.

Ключи нужно хранить в защищенном хранилище, таком, что любая неавторизованная попытка считать ключи неизбежно приведет к обнулению этого хранилища.

Ключи должны быть защищены в момент передачи между шифраторами.

Поэтому при передаче ключи всегда должны зашифровываться. Каждый шифратор имеет свой собственный сертификат, выданный удостоверяющим центром.

Процесс обмена ключами использует сертификат для подписи ключей или частей ключей, которыми обмениваются для того, чтобы убедиться, что они получены от правильного удаленного устройства.

Частичные ключи генерируются целиком внутри шифратора, и при этом никакой пользователь не имеет доступа к ним.

Обменявшись частичными ключами, обе стороны вычисляют тот же самый разделяемый секрет. После этого шифратор генерирует внутри себя мастер-ключ, и шифрует его разделяемым секретом. Шифратор также генерирует ключ сеанса и шифрует его с помощью мастер-ключа.

Передача мастер-ключа и ключей сеанса от одного шифратору к другому всегда происходит в зашифрованном виде.

Для обмена мастер-ключами обычно используются два самых распространенных алгоритма асимметричного шифрования, **RSA** и **ECC** (Elliptic Curve Cryptography, криптография на эллиптических кривых).

Шифрование на 2-м уровне сети

Сети передачи данных 2-го уровня (то есть с коммутацией кадров по MAC-адресам) обеспечивают пропускную способность и время отклика, которые не могут обеспечить сети 3-го уровня. Они также позволяют использовать широкий набор сетевых топологий, недостижимый на 1-м уровне. Вот почему крупные компании и государственные организации предпочита-

ют сетевые технологии 2-го уровня для своих критически важных высокоскоростных городских и глобальных сетей. **Проще говоря, сети 2-го уровня отличаются простотой, существенно более низким временем отклика, удобством управления, гибкостью и расширяемостью.**

Однако тогда, когда необходимо внедрить сетевой шифрование, экономические преимущества сетей 2-го уровня становятся особенно заметными. Ведь в них можно реализовать шифрование на этом же, то есть 2-м уровне сетевой модели. Именно этот подход обеспечивает оптимальный баланс между эффективностью шифрования и гибкостью в построении сетей, что дает экономию и снижение совокупной стоимости владения решением для шифрования.

Устройства, реализующие доверенное шифрование в городских и операторских сетях Ethernet, образуют отдельный класс высокоскоростных шифраторов. Они отличаются следующими особенностями:

Они используют для реализации функции шифрования программируемые логические интегральные схемы (ПЛИС), которые обеспечивают оптимальный баланс между производительностью и гибкостью, обеспечивают стабильную работу под нагрузкой и позволяют избежать потерь информации. Системы, построенные на базе универсальных ЦП или, наоборот, специализированных заказных микросхем, проигрывают.

Шифрование кадров Ethernet в транспортном режиме с аутентификацией заголовков (для имитозащиты) гарантирует низкие накладные расходы пропускной способности сети на передачу дополнительной информации. Распространенные решения на базе протоколов IPSec используют туннелирование и добавляют много дополнительной информации. Поэтому расход пропускной способности сети возрастает, особенно при трафике, состоящем из маленьких пакетов (например, интерактивной голосовой связи или запросов к базам данных).

Вносимая задержка минимальна, так как устройства работают в сквозном режиме коммутации, то есть начинают шифровать кадр еще до того, как он полностью принят. Это очень важно для разных классов приложений. Например, для сетевых архитектур с использованием ЦОД-ов задержка является ключевым параметром. Криптошлюзы, шифрующие данные на 3-м или более высоких уровнях, вносят существенную задержку.

Такие устройства очень просто встраивать в сеть. Они обычно устанавливаются на стыке между оконечным оборудованием городской сети и кампусной сетью, имеют 2 физических порта Ethernet и устанавливаются по принципу «врезки в линию», то есть просто пропускают трафик через себя в обеих направлениях (или не пропускают, или шифруют), прозрачны для служебных протоколов 2-го и более высоких уровней. Тем самым снижается риск ошибки персонала, особенно если оператор шифратора не занимается администрированием всей сети на ежедневной основе. Изменения в адресации (добавление узлов и подсетей, изменения) никак не сказываются на их работе и не требуют никакого переконфигурирования (в отличие от решений на базе IPSec, где в таких случаях может потребоваться обновлений в политиках безопасности IPSec).

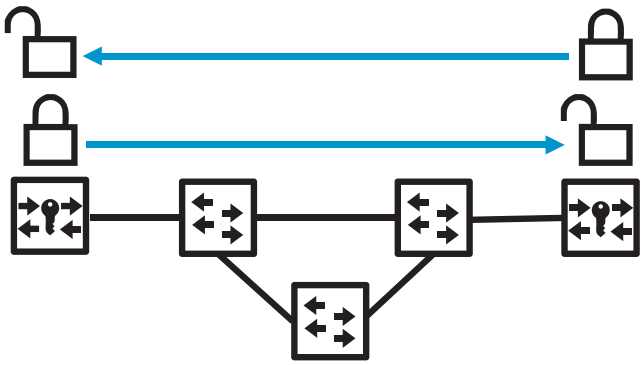


Рис. 4 Сквозное шифрование

Может получиться так, что сеть использует на своем протяжении не только технологии 2-го уровня (коммутацию Ethernet), но и другие технологии, например, MPLS. Но и в этом случае есть решение: шифратор второго уровня оставляет служебную информацию, необходимую для коммутаторов MPLS, незашифрованной, с тем, чтобы они могли распознавать и обновлять ее.

Использование технологий Carrier Ethernet обеспечивает гибкость в топологиях. Такие устройства могут работать не только в конфигурации «точка-точка» (то есть парами), но и в других топологиях («точка-многоточка», или «корень и листья» с одним центральным узлом и несколькими периферийными, или же «многоточка-многоточка» – такие топологии требуются для поддержки распространенных сценариев подключения. Шифраторы 1-го уровня сети (также называемые канальными шифраторами) не обладают такой гибкостью.

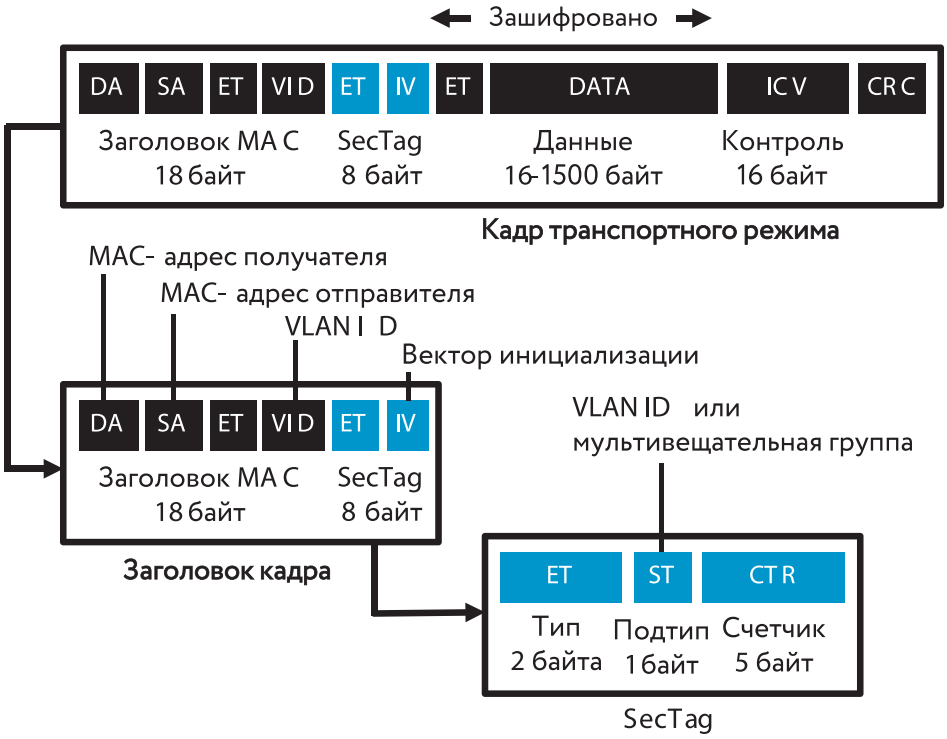
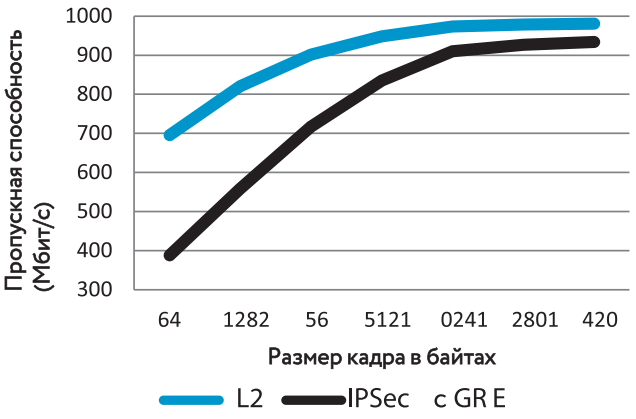


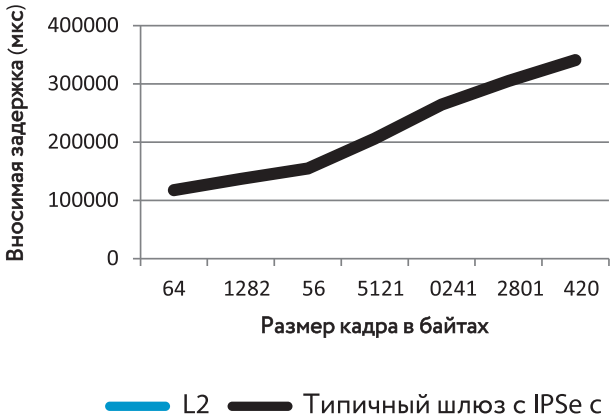
Рис. 5 Формат кадра транспортного режима, сравнение производительности при шифровании на 2-м и 3-м уровнях

Рис. 6 Шифрование L2 в равнении с IPSec

Эффективная пропускная способность



Вносимая сетевая задержка



Высокоскоростные шифраторы «Палиндром»

В сегодняшнем мире, где невозможно физически контролировать все свои данные, а из-за их огромных объемов последствия утечек могут быть катастрофическими, **«СИС Крипто»** позволит уберечься от кражи конфиденциальной информации благодаря простым в использовании разработанных для местного рынка продуктам мирового уровня.

В частности, **«СИС Крипто»** производит в России и предлагает на российском рынке высокоскоростные шифраторы семейства **ВСШ «Палиндром»**. Они предназначены для шифрования высокоскоростных каналов в городских сетях на базе Ethernet. Высокоскоростные шифраторы Ethernet компании **«СИС Крипто»** реализуют доверенное шифрование на 2-м уровне сети.

Сделаны в России на базе платформы шифрования мирового класса и криптомодуля отечественной разработки. Используется алгоритм шифрования ГОСТ Р 34.12-2015 с длиной блока 128 бит. Отличаются оптимальным сочетанием производительности, стабильности работы и гибкости благодаря использованию программируемой логической интегральной схемы (ПЛИС). **Так как устройства предназначены исключительно для шифрования, риск ошибок при их развертывании и сопровождении минимален.**

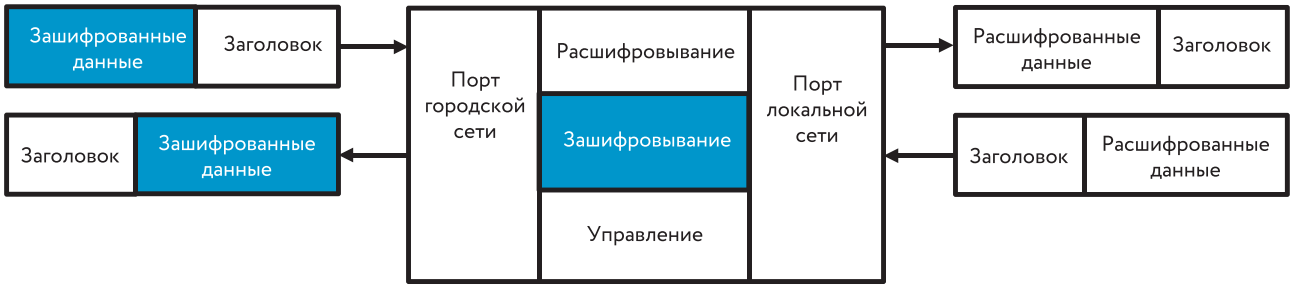


Рис.7 Принцип работы шифратора

Высокоскоростные шифраторы СИС Крипто обладают всеми качествами доверенного шифрования:

- Специализированное, защищенное от физического взлома и недоверенной загрузки оборудование.
- Централизованная автоматическая система управления ключами шифрования.
- Сквозное аутентифицированное шифрование.
- Криптозащита на базе алгоритмов ГОСТ.

Семейство высокоскоростных шифраторов СИС Крипто обеспечивает максимум защиты данных без ущерба для производительности приложений, и представляют собой наращиваемое решение, пригодное для всех протоколов и топологий 2-го уровня сети.

- Работа на скорости линии.
- Практически нулевые вносимые задержки и накладные расходы на полосу пропускания.
- Наращиваемость, которая позволяет удовлетворить растущие требования к пропускной способности.
- Настроил и забыл» – простота начальной настройки и управления.
- Полная совместимость между шифраторами разных моделей
- Выдающийся уровень готовности 99,999%.
- «Врезка в линию» – установка и настройка без вмешательства в работу других сетевых устройств.

ВСШ «Палиндром» 6000-й серии
Шифраторы корпоративного класса, предназначенные для шифрования данных в опорных сетях организации и в любых других случаях с высокими требованиями к пропускной способности. Они оснащены дублированными блоками питания и вентиляторами, снабжены дисплеем и кнопками на передней панели, устанавливаются в 19-дюймовую стойку.

ВСШ «Палиндром» 4000-й серии
Предназначены для шифрования транспортных сетей подключения филиалов, а также для любых других сценариев с умеренными требованиями к пропускной способности. Она выпускаются в компактном настольном корпусе, допускающем также установку в 19-дюймовую стойку. Они совместимы с шифраторами 6000-й серии.

Сравнительные характеристики моделей ВСШ «Палиндром»

МОДЕЛЬ	4010	4020	6140
СЕТЕВЫЕ ПРОТОКОЛЫ И ИНТЕРФЕЙСЫ			
Все топологии Carrier Ethernet	+	+	+
Максимальная скорость	1 Гбит/с	1 Гбит/с	1 Гбит/с
Выбор скорости канала	+	+	+
Поддержка Jumbo Frames	+	+	+
Автоматический поиск и установка соединения между шифраторами	+	+	+
РАЗЪЕМЫ			
Внутренняя сеть	1 x RJ45	1 x SFP или SFP+	1 x SFP или SFP+
Внешняя сеть	1 x RJ45	1 x SFP или SFP+	1 x SFP или SFP+
Управление out-of-band	1 x RJ45	1 x RJ45	1 x RJ45
Консоль	1 x RJ45 RS-232	1 x RJ45 RS-232	1 x RJ45 RS-232
Загрузка микрокода	1 x USB	1 x USB	1 x USB
БЕЗОПАСНОСТЬ			
Защита от вскрытия корпуса	+	+	+
Защита от зондирования	+	+	+
Защита от недоверенной загрузки	+	+	+
Режимы сетевого протокола шифрования	транспортный туннельный	транспортный туннельный	транспортный туннельный
Методы передачи шифруемого трафика	однонаправленный широковещательный мультивещательный	однонаправленный широковещательный мультивеща- тельный	однонаправленный широковещательный мультивещательный
Выборочное шифрование	по MAC-адресам или VLAN ID в сочетании с EtherType и методом передачи	по MAC-адресам или VLAN ID в сочетании с EtherType и методом передачи	по MAC-адресам или VLAN ID в сочетании с EtherType и методом передачи
Имитозащита	+	+	+
Защита от анализа трафика (TRANSEC)	+	+	+
Централизованное автоматическое управление ключами	+	+	+

МОДЕЛЬ	4010	4020	6140
Алгоритм шифрования	ГОСТ Р 34.12-2015	ГОСТ Р 34.12-2015	ГОСТ Р 34.12-2015
Длина ключа	128 бит	128 бит	128 бит
ПРОИЗВОДИТЕЛЬНОСТЬ			
Полнодуплексное шифрование на скорости линии с минимальными накладными расходами пропускной способности	+	+	+
Архитектура со сквозной коммутаций на базе ПЛИС	+	+	+
Типичная вносимая задержка, мкс	<10 на 1 Гбит/с <50 на 100 Мбит/с <650 на 1 Мбит/с	<10 на 1 Гбит/с <50 на 100 Мбит/с <650 на 1 Мбит/с	<5 на 10 Гбит/с <10 на 1 Гбит/с <50 на 100 Мбит/с <650 на 1 Мбит/с
УПРАВЛЕНИЕ			
Каналы управления	Ethernet in-band Ethernet out-of-band консоль	Ethernet in-band Ethernet out-of-band консоль	Ethernet in-band Ethernet out-of-band консоль
Настройка	SNMPv3 или консоль	SNMPv3 или консоль	SNMPv3 или консоль
Мониторинг	SNMPv1/2/3 или конс.	SNMPv1/2/3 или конс.	SNMPv1/2/3 или конс.
Формат сертификатов	X.509v3	X.509v3	X.509v3
Поддержка внешних удостоверяющих центров	+	+	+
Поддержка серверов времени NTP	+	+	+
РАЗМЕРЫ, МАССА, УСЛОВИЯ ЭКСПЛУАТАЦИИ			
Размеры (Ш / В / Г), мм	180 / 32 / 126	180 / 32 / 126	435 / 43 / 329
Масса, кг	0,5	0,5	8,5
Тип корпуса	настольный или 1U	настольный или 1U	1U
Блок питания	внешний	внешний	встроенный дублированный
Мощность при полной нагрузке, Вт	10	11	50
Вентилятор	-	+	дублированный
Температура и влажность	0-80 %, до 40 °C	0-80 %, до 40 °C	0-80 %, до 50 °C

СИС Крипто

«СИС Крипто» предлагает на российском рынке высокоскоростные шифраторы семейства «Палиндром» для криптозащиты городских сетей на базе технологий Metro и Carrier Ethernet.
www.ciscrypto.ru

CIS / № 1 (7) / 2019 / www.cismag.ru

Выставка «Открытый музей-2019»

Выставка «Открытый музей-2019» – продолжение «Антимузея», проекта, стартовавшего в 2016 году, и функционировавшего как свободная площадка для творческого высказывания без жанровых и кураторских ограничений.

Цель проекта – показать актуальные тренды современного медиа- и технологического искусства и смежных пространств творческого высказывания, способствовать их развитию.

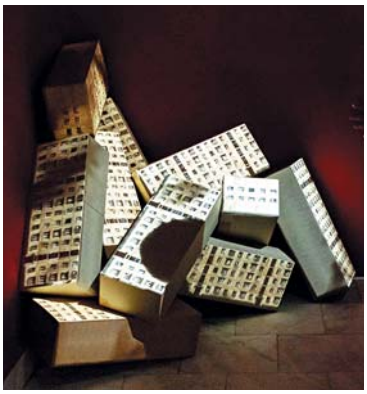
На выставке будут показаны все поданные проекты, если они удовлетворяют одному или нескольким из критериев, определяющих современное медийное и технологическое искусство – интерактивные инсталляции и объекты, дополненная реальность, машинимы, видео, аудиовизуальные перформансы, документация интервенций в городской среде, артистические модификации компьютерных игр и программ, 3D глитчи, и другое.

КРИПТОГРАФ (рис. 1) – интерактивный объект Владлены Громовой и Артёма Парамонова.

«Криптограф» – синтезатор, надстраивающий звуковое измерение над небольшим предметам и изображениям. Инструмент задействует эстетический потенциал пограничных областей, объединяет признаки разных эпох и систем: традиционную западноевропейскую теорию музыки и код, свойства человеческого и нечеловеческого, визуального и звукового. Синтезатор состоит из камеры, компьютера, сенсорного экрана, кода, деревянного корпуса и акустической системы. Камера захватывает картинку и/или предмет, размещённые на корпусе инструмента, и по заданному алгоритму синтезатор интерпретирует изображение в звук.

Алгоритм основан на двух гипотезах.

Первая – предложена художницей Кэтрин Любар, которая проводит аналогию между психофизиологической оценкой музыкальных интервалов и цветовых сочетаний.



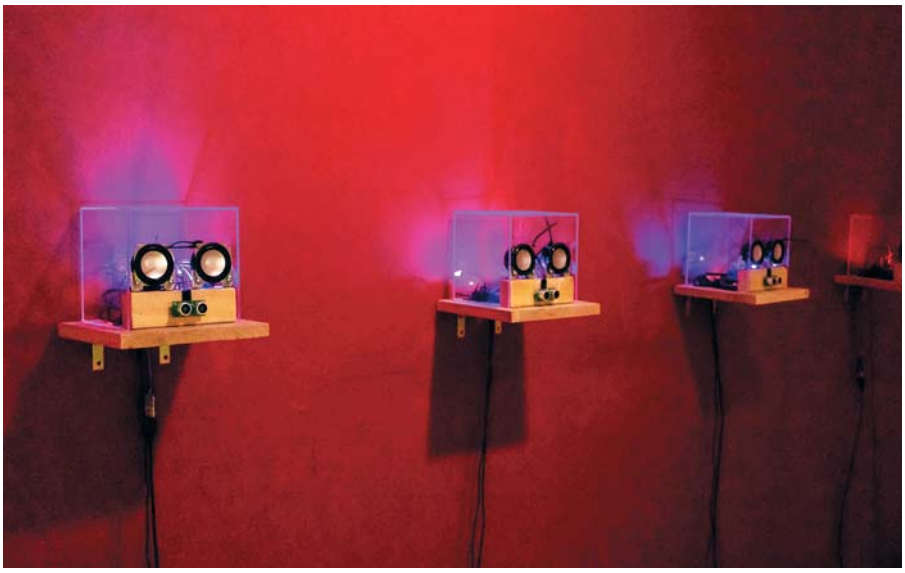


Рис. 2 «Трафик»

Рис. 1 «Криптограф»

Вторая гипотеза о существовании ранжира восприятия элементов изображения зрительным анализатором человека выведена изобретателем Николаем Блиновым. Этот ранжир и определяет последовательность считывания изображения.

ТРАФИК (рис. 2), Интерактивная инсталляция. Дмитрий Ольгин.

Это работа о захвате внимания/пространства в какой-то мере с архитектурной точки зрения. О проблеме давления множества факторов и обстоятельств, мешающих сконцентрироваться на чём-то действительно важном.

Коллекция звуков, входящих в наш каждодневный фон (объявления, реклама), выставлена на «прилавке» в виде кастомных колонок. Каждая из них звучит отдельно. Тем самым этот «киоск» погружает нас в то самое неопределенное состояние спора на совещании, гула на рынке, или просто в ситуацию, когда нам нужно выбрать один из сотни видов печенья в магазине.

Но у зрителя есть возможность противостоять этим раздражителям физически, с помощью собственного тела, перекрывающего звук одной из колонок по выбору. Датчик расстояния в каждой колонке следит за положением зрителя напротив и выключает звук с приближением человека.

ВЫСТАВОЧНЫЕ ОБЪЕДИНЕНИЕ ЗАЛЫ МОСКВЫ
ЭЛЕКТРО МУЗЕЙ

Кураторы Электромузея:
Алексей Шульгин; Аристарх Чернышев

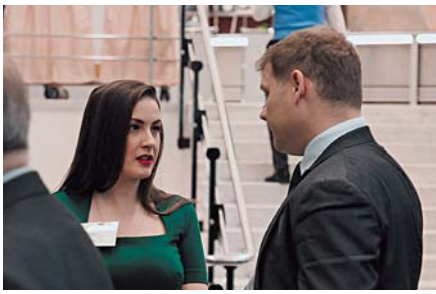
Место проведения:
«Электромузей в Ростокино»
(Ростокинская ул., 1, м. ВДНХ,
МЦК «Ростокино»)
Тел: 8 (499) 187-10-45;
electromuseum@vzmoscow.ru
www.vzmoscow.ru


Управлени
зационно-техническими мероприятиями
по защите ин
и в организации, муниципалитете, ре
CIS


Й РЕГИОН СУЩЕСТВУЕТ!
digit.

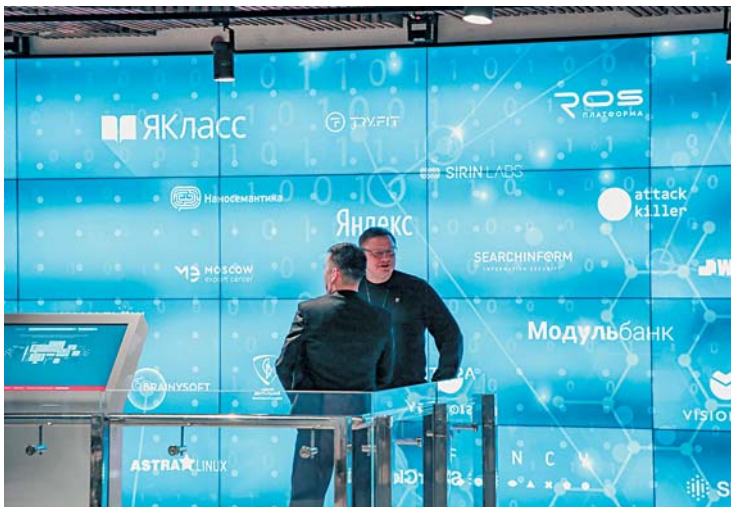

Основы
Новый уче
Проек
DevOps
Новая


Цифровой
Форум
2019




ТНЫЙ РЕГИОН СУЩЕСТВУЕТ!
ЛАТФОРМА DIGIT - ОСНОВА ПРОЕКТА "УМНЫЙ РЕГИОН"
digit.
П 2000
Digital Forum

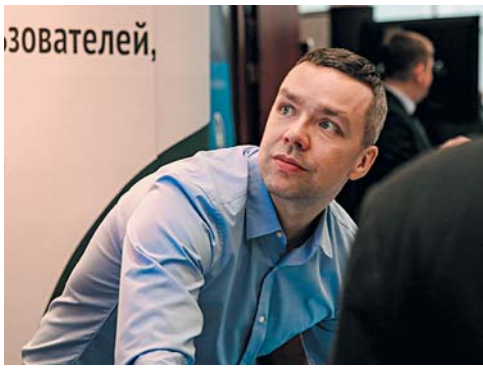

ЦИФРОВАЯ
ТРАНСФОРМАЦИЯ
и ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ РОССИИ


ЯКласс
ROS
ПЛАТФОРМА
TRY.FIT
SIRIN LABS
Наносемантика
Яндекс
attack killer
SEARCHINFORM
MOSCOW
Модульбанк
BRAINYSOFT
ASTRA LINUX


Moscow
Digital
Forum


Мария Алехина

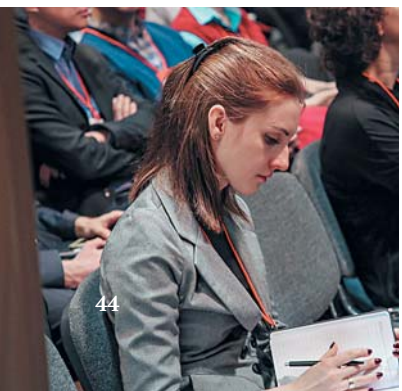

ИНФО
ФОРУМ
2019




ВЭБ
БАНК
РАЗВИТИЯ

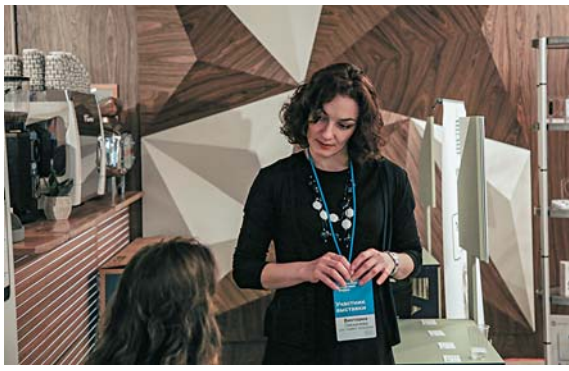

COMMVAULT
Современный
Превратите
информацию в
стратегический
актив.
COMMVAULT

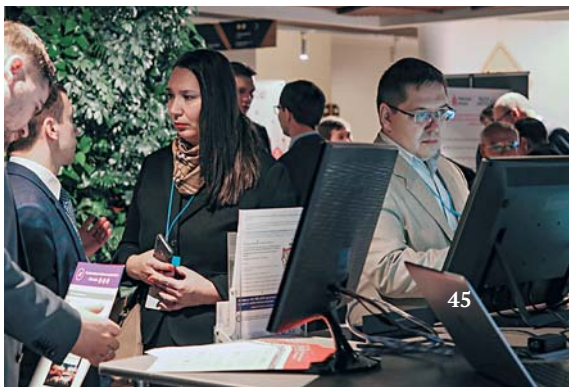

ДиалогНаука




WireGeo
BP КОНЦЕПТ


GConf.Russia
2019

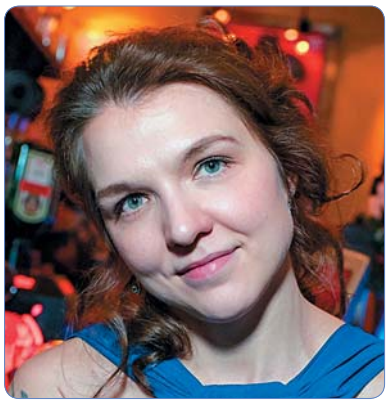




Кроссворд «Мисс CIS»

Отгадайте имена и фамилии девушек работающих в ИТ-сфере, отправьте фото разгаданного кроссворда на почту info@sovinfosystems.ru и получите приз от редакции журнала «CIS».

В первой строке – имя,
во второй – фамилия.



Подсказки на сайте
www.cismiss.ru

Календарь мероприятий

1-30 апреля
Томск • Онлайн-трансляция • Курс
Машинное обучение

1-5 апреля
Москва • Курс
DSAV: Анализ данных и визуализация в R

2-4 апреля
Москва • Онлайн-трансляция • Конференция
TestCon Moscow 2019

2 апреля - 3 июня
Санкт-Петербург • Курс
DevOps Engineer

3 апреля
Москва • Хакатон
HR STARTUP COMPETITION

4 апреля
Новосибирск • Конференция
Код ИБ Новосибирск

4 апреля
Москва • Конференция
InoThings++

4 апреля
Онлайн-трансляция • Вебинар
Управление талантами на платформе 1С: Предприятие: оценка персонала по компетенциям, управление развитием персонала и кадровый резерв

5 апреля
Москва • Онлайн-трансляция • Конференция
Moscow Python Conf

5-6 апреля
Санкт-Петербург • Тренинг
Мотивация и коучинг IT-команды

5-6 апреля
Санкт-Петербург • Курс
Visio моделирование. Визуализация данных в Visio. Инфографика

5 апреля
Онлайн-трансляция • Конференция
Digital-конференция MEET FOR SPEED

6 апреля
Минск • Конференция
RubyConfBY 2019

8-9 апреля
С.-Петербург • Онлайн-трансляция • Конференция
Saint Highload++

8-12 апреля
Москва • Конференция
IEEE FRUCT 2019: 24th Conference of Open Innovations Association FRUCT

9 апреля
Москва • Конференция
AI Conference

9 апреля - 16 мая
Новосибирск • Курс
Курс Java Developer

10-14 апреля
Киев • Тренинг
Комплексный тренинг по бизнес-анализу (по BABOK 3.0)

10-12 апреля
Москва • Курс
BDAM: Аналитика больших данных для руководителей

10 апреля
Санкт-Петербург • Мастер-класс
Психология изменений

11 апреля
Баку • Конференция
Код ИБ Баку

11 апреля
Москва • Конференция
Конференция «Цифровизация в агробизнесе»

11 апреля - 23 мая
Онлайн-трансляция • Курс
Фундаментальный курс по SEO

12 апреля
Москва • Конференция
IV Fresh Russian Communications Conference 2019

13 апреля
Москва • Турнир
Турнир по шахматам «IT Chess Moscow 2019»

13 апреля
Москва • Митап
JetBrains Night Moscow 2019

14 апреля
Москва • Турнир
Турнир по настольному теннису «IT Match Point Moscow 2019»

15-18 апреля
Москва • Курс
HBASE: Администрирование кластера HBase

16 апреля - 24 мая
Новосибирск • Онлайн-трансляция • Курс
Курс web-разработки (backend) на Python

16 апреля
Москва • Конференция
Телеком 2019

18 апреля
Краснодар • Конференция
Код ИБ Краснодар

18 апреля
Москва • Конференция
E. DAY 2019. Встраиваемые Технологии и Интернет Вещей

18 апреля
Prague • Конференция
Prague iGaming & Affiliate Conference

18 апреля
Москва • Митап
Panda-Meetup. Frontend

19 апреля
Екатеринбург • Конференция
Конференция уральских разработчиков DUMP-2019

19-20 апреля
Пенза • Конференция
SECON»2019

20 апреля
Харьков • Онлайн-трансляция • Конференция
NODE»19

20-21 апреля
Киев • Тренинг
Тренинг Leading SAFe® 4.6

20 апреля
Москва • Онлайн-трансляция • Форум
DevOpsForum 2019

20 апреля
Екатеринбург • Онлайн-трансляция • Форум
Global Business Forum

20-21 апреля
Киев • Фестиваль
WEGAME 5.0

22-23 апреля
Москва • Онлайн-трансляция • Конференция
Apps Conf

22-23 апреля
Москва • Форум
XI Межотраслевой Форум «CISO FORUM: кулинарная книга CISO»

23-24 апреля
Сингапур • Форум
Blockchain Life 2019

24 апреля
Минск • Конференция
Minsk iGaming Affiliate Conference

25-26 апреля
Alicante • Выставка
International Digital Summit & Expo D1

25 апреля
Онлайн-трансляция • Вебинар
Автоматизация управления по целям и KPI в среднем и крупном бизнесе

26-27 апреля
Ульяновск • Конференция
VIII Международная IT-конференция «Стачка»

26 апреля
Москва • Онлайн-трансляция • Конференция
KnowledgeConf

26-27 апреля
Санкт-Петербург • Конференция
HR API 2019

26 апреля
Минск • Конференция
Конференция RAUX

27 апреля - 2 мая
Билярск • Курс
Весенний лагерь «Sanak-lab»

Мисс CIS

ИТ-конкурс красоты

Всероссийский ежегодный конкурс красоты
среди девушек работающих в ИТ-сфере.

Миссия конкурса – выявить самых красивых девушек
на звание «Мисс CIS» и создать из обладательницы короны
символ информационной безопасности России.

CIS Современные Информационные Системы

www.cismiss.ru