CIS
Современные Информационные Системы
№ 3 (5) / 2018

БИЗНЕС С НУЛЯ В РОССИИ

Стр. 4

Русский софтъ

«Продукты» и «Решения»

Как развиваются ключевые тренды на ИТ-рынке?

Стр. 8

ПРЕДИСЛОВИЕ

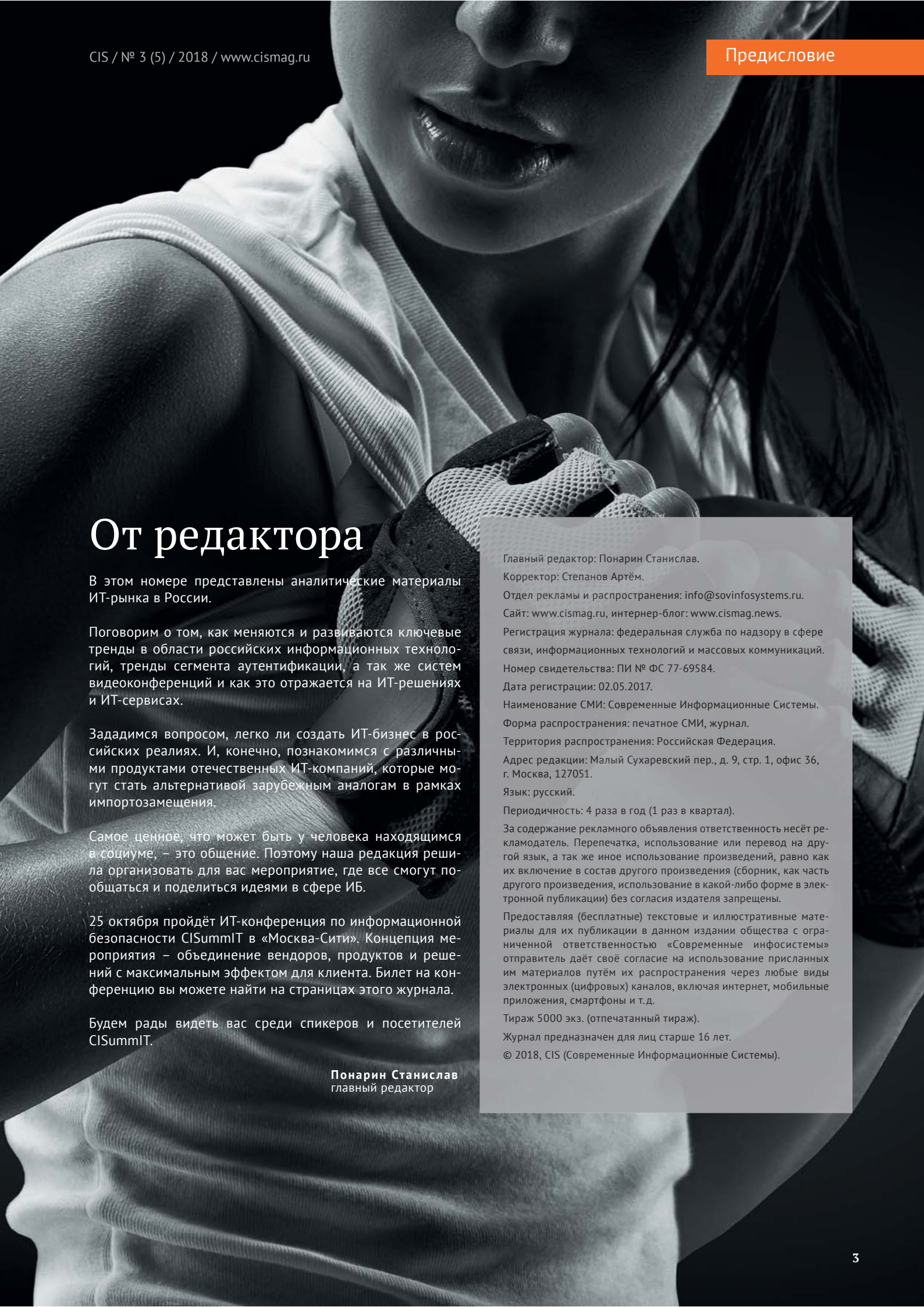
ОПЫТ

ПРОДУКТЫ

АНАЛИТИКА

РЕШЕНИЯ

КАЛЕНДАРЬ



От редактора

В этом номере представлены аналитические материалы ИТ-рынка в России.

Поговорим о том, как меняются и развиваются ключевые тренды в области российских информационных технологий, тренды сегмента аутентификации, а так же систем видеоконференций и как это отражается на ИТ-решениях и ИТ-сервисах.

Зададимся вопросом, легко ли создать ИТ-бизнес в российских реалиях. И, конечно, познакомимся с различными продуктами отечественных ИТ-компаний, которые могут стать альтернативой зарубежным аналогам в рамках импортозамещения.

Самое ценное, что может быть у человека находящимся в социуме, – это общение. Поэтому наша редакция решила организовать для вас мероприятие, где все смогут пообщаться и поделиться идеями в сфере ИБ.

25 октября пройдёт ИТ-конференция по информационной безопасности CISummIT в «Москва-Сити». Концепция мероприятия – объединение вендоров, продуктов и решений с максимальным эффектом для клиента. Билет на конференцию вы можете найти на страницах этого журнала.

Будем рады видеть вас среди спикеров и посетителей CISummIT.

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: Малый Сухаревский пер., д. 9, стр. 1, офис 36, г. Москва, 127051.

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.

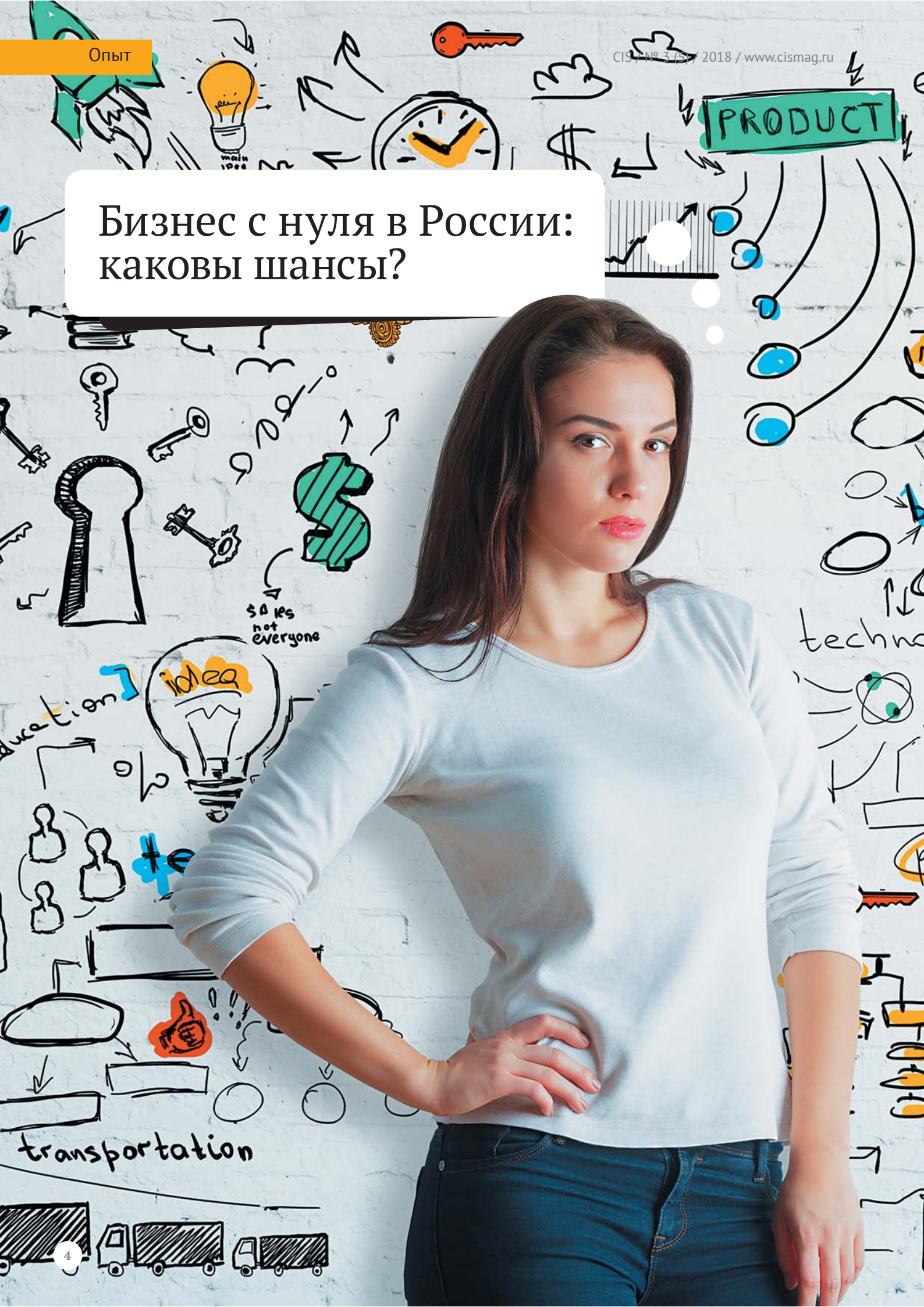
Предоставляя (бесплатные) текстовые и иллюстративные материалы для их публикации в данном издании общества с ограниченной ответственностью «Современные инфосистемы» отправитель даёт своё согласие на использование присланных им материалов путём их распространения через любые виды электронных (цифровых)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

Тираж 5000 экз. (отпечатанный тираж).

Журнал предназначен для лиц старше 16 лет.

© 2018, CIS (Современные Информационные Системы).

Бизнес с нуля в России: каковы шансы?



Возможно ли создать бизнес в этой стране с нуля? А если он инновационный и качественный? А с оборудованием? А когда основными клиентами являются B2B и крупные предприятия? Можно ли изменить образ жизни и выяснить, где больше всего самых состоятельных клиентов?

В стране стартует множество программ поддержки высокотехнологичных компаний: технопарк, акселераторы, государственные субсидии, конкурсные торги и т.д. Но барьеры для входа высокие и волокита, непоследовательные трактовки правил, запутанные условия участия и отчётности съедают драгоценное время вашей команды. И, прежде всего, серьезные конкуренты также не лучшим образом влияют на ещё хрупкое предприятие.

Мы составили 5 постулатов для достижения цели и продолжаем фокусироваться на них. Но и о книгах точно не стоит забывать.

Сотрудничество с клиентами и партнёрами B2B на ранней стадии разработки продукта. Крупные заказчики руководствуются не новыми решениями, а старыми, так как они стремятся к стабильности. Им не нужен ваш MVP-продукт (минимально жизнеспособный продукт). Именитые поставщики засыпают вас вопросами об SLA для гарантии жизнеспособности компании. Вот что вам нужно. Спуститесь на землю, обивайте пороги и стойте на своём, напомните, что вы пришли за советом. В наших реалиях непросто получить обратную связь, но все хорошо знают, насколько это важно. К счастью, сегодня в большом бизнесе появляется тенденция обращаться за советами, так как стало важнее поднять продукт вместе, пользуясь советами и помощью. Системные интеграторы будут с вами. Создать новые решения, ориентированные на клиентов, возможно только при помощи стартап-интегратора. Так как у них взгляд шире, а у вас более свежий. Десегментация ИТ-рынка, как и диверсификация бизнеса, играют на руку. Например, в банках и телекоммуникационных компаниях по всему миру наступил кризис, так как их услуги и предложения устарели.

Совершенство в коммуникации. Ограниченность ресурсов простительна, но не ваше исчезновение. Начиная с самой первой связи, сообщения, презентации продукта и изготовления информационных материалов следует учитывать каждую мелочь. Второго шанса не будет. Клиенты по всему миру избалованы международными вендорами, и им будет приятно, если вы будете поддерживать высокий уровень коммуникации и предлагать качественный информационный материал и услуги.

Глобализация с самого зарождения. Не стоит рассчитывать на импортозамещение, так как это касается лишь военных и других ключевых предприятий. Поэтому в других случаях очень важно постоянно увеличивать качество и функциональность продукции. Кроме всего прочего, международный рынок играет роль цензора качества. Проверка конкурентоспособности и мониторинг реакций потребителей крайне необходимы и могут осуществляться при поддержке РЭЦ и «Руссофт». Ориентация на международные стандарты будет полезна и на отечественном рынке— она позволит бизнесу жить не только сегодня, но и завтра.

Мария Рукавишникова
основатель и CEO
Getmobit

Ум и сообразительность: баланс между строгой дисциплиной и творческим духом команды. Важны оба. Как внедрять инновации без творчества? сообразительность и креативность, продуманные практики должны применяться в компании на всех уровнях, а не только где-то в недрах отдела разработки. Многим топ-менеджерам действительно стоит изменить свой образ мышления. Командный поиск также проблемный вопрос. Российский менталитет можно покорить только бескомпромиссными высокими требованиями к ресурсам, процессам и ценностям (стандартам) компании.

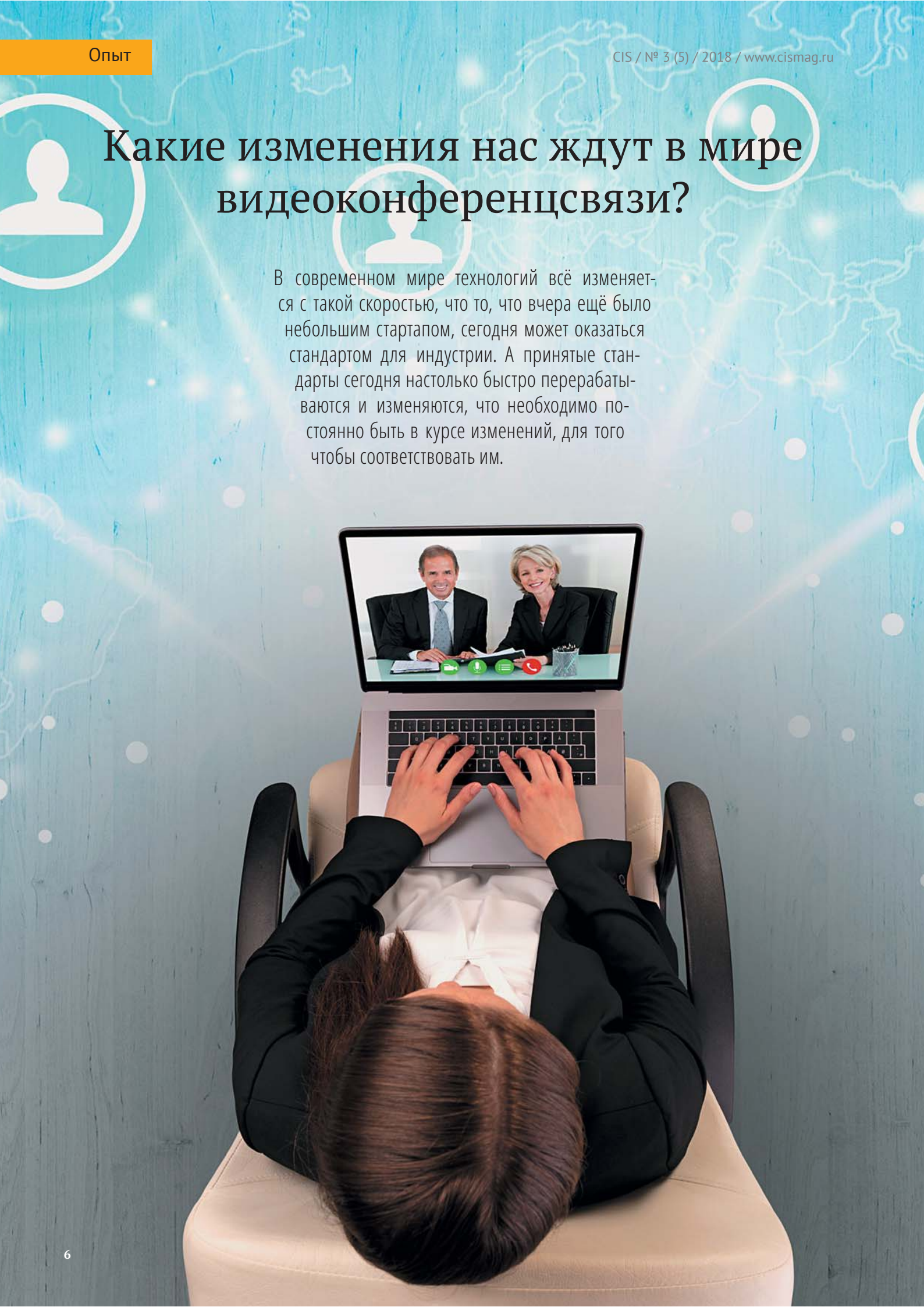
Аналитика: новое, как раньше. Чем обычно занимается в компании аналитик? Составляет перечень работ, если того требуют клиенты. Но ваша команда отвечает за новый продукт? Перечень работ и условия постоянно меняются! Чтобы выжить на рынке, необходимо учитывать всё: современные и устаревшие технологии, изменения технологических трендов и технических стандартов, коммерческие и политические аспекты, а также анализировать клиентуру и конкуренцию даже в смежных областях. В компании каждый должен быть аналитиком.

Бизнес – это всегда битва, выбор лучшего из доступного, но не всегда достаточно хорошего, и именно огромное стремление к вышеупомянутым принципам позволяет инновационным компаниям на ранней стадии существования справляться с трудностями из-за стремительно растущих требований конъюнктуры рынка, преодолевать все преграды и превращать угрозы в сильные конкурентные преимущества.

Мария Рукавишникова

Какие изменения нас ждут в мире видеоконференцсвязи?

В современном мире технологий всё изменяется с такой скоростью, что то, что вчера ещё было небольшим стартапом, сегодня может оказаться стандартом для индустрии. А принятые стандарты сегодня настолько быстро перерабатываются и изменяются, что необходимо постоянно быть в курсе изменений, для того чтобы соответствовать им.



Сейчас уже никого не удивляет видеоконференцсвязь, хотя несколько лет назад казалось, что это привилегия для топ-менеджеров больших компаний, но сейчас любой рядовой сотрудник может беспрепятственно воспользоваться ВКС для связи со своими коллегами. Отрасль ВКС продолжает активно расти и развиваться. Так какие же изменения нас ждут в мире видеоконференцсвязи?

Видеосвязь где угодно

Прошли времена когда для того, чтобы связаться с коллегами из другого города, нужно было набиваться большой кучей в комнату на другом конце офиса, оборудованную видеотерминалом, чтобы провести короткое совещание, где больше времени тратилось на подготовку, чем на само общение. Теперь у нас есть возможность учувствовать в видеоконференциях не только из переговорных комнат и рабочих мест, а буквально, откуда угодно, благодаря мобильным устройствам. Собеседование в кафе с планшета и деловые переговоры в транспорте с телефона скоро станут обыденностью и позволят экономить кучу времени и всегда быть на связи, несмотря на все препятствия. И индустрия уделяет значительное внимание мобильным платформам, и появляются решения как от небольших компаний, предлагающих свои приложения для мобильных, таких как Zoiper или Bria, так и гигантов вроде Cisco – с приложениями Jabber и WebEx – или Polycom со своим RealPresence. Не отстают и мессенджеры, добавляющие поддержку видео в свои приложения. Сейчас для видеозвонков можно использовать Skype, Facebook Messenger, Google Duo, Google Hangouts, WhatsApp, Viber, Imo – и этот список постоянно растёт.

Видеоконференции в «облаках»

Сейчас всё сильнее и сильнее развивается модель SaaS (Software as a Service), когда поставщик услуги размещает всё на своих мощностях и предоставляет пользователю удалённый доступ. Это удобно, потому что пользователю не нужно закупать оборудование для видеоконференций, создавать инфраструктуру и иметь специализированный персонал который будет следить за этим всем. Гораздо проще, особенно для небольших компаний, платить ежемесячную плату, которая будет в разы меньше, чем стоимость покупки и развёртывания серверов для ВКС, и сразу получить готовый сервис с технической поддержкой. Например, сейчас популярны сервисы от компаний Zoom, Polycom, Cisco WebEx, но появляется всё больше небольших компаний, которые способны представить достойную конкуренцию текущим участникам рынка. Одним из таких новых участников может стать набирающий популярность сервис appear. in, позволяющий совершать видеозвонки через браузер, используя технологию WebRTC.

Рост видеотрафика

Процент коммуникаций с использованием видеоконференций неуклонно растёт с каждым годом. Растёт число пользователей, передающих видеотрафик, увеличивается качество картинки и звука, и поэтому при проектировании сетевых инфраструктур нужно учитывать что видеотрафик, который очень сильно чувствителен к задержкам и потерям, будет продолжать расти. Также нужно подстраиваться к изменениям и провайдерам – клиенты будут уходить, если на видеоконференциях будет разваливаться картинка и пропадать звук. При этом есть ещё видеохостиги, стриминговые площадки, онлайн-кинотеатры и прочие ресурсы, основным контентом у которых является видео, и их количество продолжает расти. В связи с этим вендоры разрабатывают оборудование, которое специально предназначено для обработки и передачи видео – такой, например, является линейка маршрутизаторов ISR (Integrated Services Router) от компании Cisco, архитектура которых предлагает мультимедийные сервисы унифицированных коммуникаций, давая возможность спроектировать сеть, готовую к росту видеотрафика.

Унификация и интеграция

Согласитесь, как было бы удобно, если бы все коммуникации мы могли бы осуществлять из одного приложения аудио- и видеозвонки, отправлять электронную почту клиенту, делиться изображением с экрана, обсуждать в чате новый проект с коллегами и чтобы всё это ещё было бы в CRM. Сейчас всё стремится к тому, чтобы либо приложения сразу включали в себя все необходимые функции, либо чтобы все отдельные части бесшовно интегрировались и у конечного пользователя создавалось впечатление единой экосистемы, без необходимости приключаться между пятью разными приложениями и ещё пятью другими, если появилась необходимость работать удалённо с мобильного устройства. Чем больше развивается технология, тем больше внимания уделяется удобству пользователей. Сейчас можно выделить решение Cisco WebEx, позволяющее делать видео- и аудиозвонки, конференции, чаты и имеющее возможность интегрироваться с большим числом приложений, таких как Google Drive, Box, Slack, Twitter, Trello, Goolgle Calendar, IFTTT, Microsoft SharePoint и другими. Или решение Polycom, предоставляющее аудио- и видеоконференции и интегрирующееся с Microsoft 356 и Skype For Business. Пока что всё это работает не совсем бесшовно и интеграция есть не таким уж и большим числом сервисов, поэтому разработчикам есть куда стремиться, а на рынке есть место для новых игроков.

Будущее видеоконференций

А какое развитие может ждать нас дальше? Отрасль видеоконференцсвязи развивается очень динамично и следит за новыми разработками в различных областях. Например, новым трендом может стать активно развивающаяся виртуальная реальность (VR), которая может вывести видеоконференции на новый уровень, создав невиданный ранее эффект присутствия. Или это могут быть нейронные сети, позволяющие изменять окружение в кадре так, чтобы создавалось впечатление, что вы находитесь в тихой переговорной комнате, а не в шумном аэропорту – для более комфортного восприятия. И поскольку видеоконференций проводится всё больше и больше, то большое внимание будет уделяться безопасности, ведь никто не хочет, чтобы их переговоры стали достоянием общественности. Нужно продолжать следить за тем, что происходит вокруг и всегда быть в курсе последних тенденций.

MERION NETWORKS

Мерион Нетворкс

Внедрение качественных и доступных ИТ-решений, направленных на повышение эффективности бизнес процессов.

www.merionet.ru

Как меняются/ развиваются ключевые тренды на ИТ-рынке, как это отражается на ИТ-решениях и ИТ-сервисах?

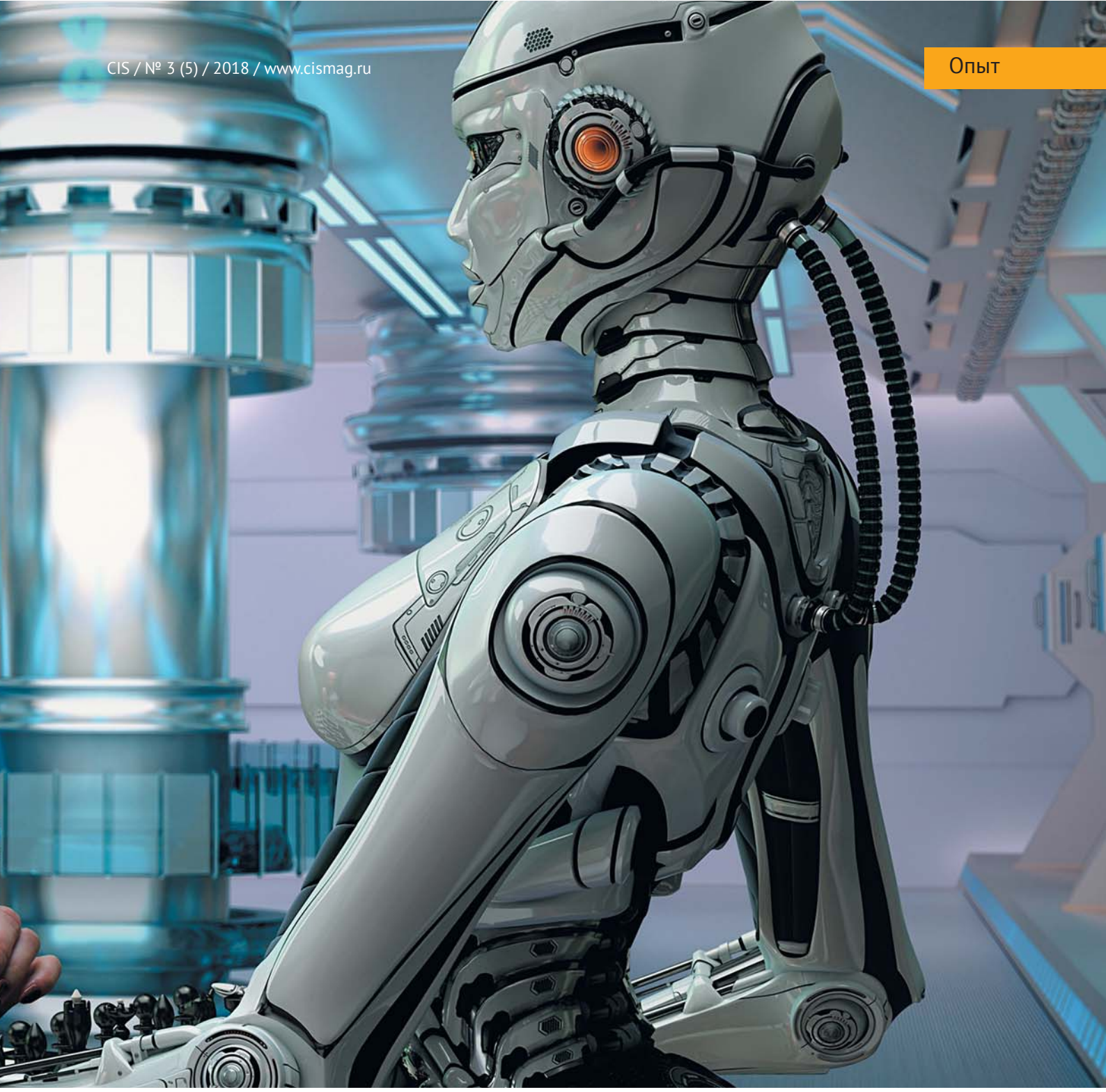
– Как меняются/развиваются ключевые тренды на ИТ-рынке, как это отражается на ИТ-решениях и ИТ-сервисах?

Сегодня погоду в ИТ-индустрии определяют два встретившихся тренда.

Первый – это огромное количество данных, ставших доступных в цифровом виде. Большинство процессов бизнеса в основном происходят в цифровом пространстве, а некоторые процессы, например финансовые, происходят целиком в виртуальном пространстве. То же и с людьми – появился огромный «цифровой след», который человек оставляет в цифровом пространстве: финансовые транзакции, оплата поездок электронными билетами, фиксация перемещений ввиду использования смартфонов и носимых устройств, попадание в область «умного» видеонаблюдения с распознаванием лиц, маршруты навигаторов и агрегаторов такси, запросы в поисковики, публикации в соцсетях и т.п. ИТ-компании накопили огромное количество таких данных, продолжают их собирать и обрабатывать.

Второй тренд – радикальное снижение стоимости вычислительных мощностей. Ещё пять лет назад вычислительные мощности и программные решения, способные решать задачи обработки больших данных, стоили миллионы долларов и их могли позволить себе только государства и международные корпорации. Сегодня те же задачи можно решать на оборудовании стоимостью до десяти тысяч долларов и программном обеспечении с открытым кодом.

Встретившись, эти два тренда породили настоящий бум систем обработки больших данных, поскольку накопилась критическая масса данных и стали доступны инструменты. Математический аппарат 300-лет-



ней давности и алгоритмы 50-летней давности, сегодня называемые «искусственным интеллектом», наконец-то стали приносить ощутимую пользу бизнесу, поэтому стали востребованы.

– Что движет рынком сегодня и что будет определять конкурентоспособность в будущем?

Состояние перманентного финансового кризиса заставляют компании оптимизировать процессы, переходить «на цифру», заменять мало- и среднеквалифицированный персонал автоматизированными системами. Поэтому те ИТ-компании, которые оседлают волну эффективности, то есть смогут предложить решения не только для автоматизации, но и для оптимизации автоматизируемых процессов, смогут вырваться вперёд. Для этого ИТ-компаниям нужно будет отойти от традиционного инфраструктурного подхода (мы продаём лучшие сервера, маршрутизаторы, СУБД и т.п.) и начать разбираться в бизнесе своих клиентов, предлагать не лучшее решение по соотношению цена/качество, а научиться мыслить так, как мыслят бизнесмены: инвестициями и их возвратом.

– Что подразумевается под умным термином: искусственный интеллект, машинное обучение?

Сегодня эти термины означают математический аппарат, позволяющий анализировать в режиме онлайн мощные потоки данных и событий, находить в них определённые, иногда неочевидные, закономерности и принимать решения в отсутствии полных данных. Это немного похоже на то, как мыслит и принимает решения на основе своего опыта и интуиции человек, поэтому такие алгоритмы называют «интеллектом». Большинство реали-

зованных в программном обеспечении алгоритмов сегодня используют математический аппарат, не выходящий за пределы университетского курса математики, поэтому никакой магии в этом нет. Сегодняшний искусственный интеллект уже может на повторяющихся процессах предсказывать определённые события лучше человека, что позволяет компаниям заменять операторов рутинных процессов на роботов, как двадцатью годами раньше автоматизировались сами эти процессы. Роботы, в отличие от людей, не болеют, не устают, не ходят в отпуск и не требуют повышения зарплаты, поэтому в процессе оптимизации процессов на возможности роботизации обращают внимание многие компании, что влечёт за собой спрос на такие разработки.

Машинное обучение (machine learning) – это один из инструментов, ассоциированных с искусственным интеллектом, чаще всего подразумевающий линейную оптимизацию данных. Другой часто упоминающийся инструмент искусственного интеллекта – «глубокое/глубинное обучение» (deep learning), или нейронные сети, обозначает нелинейные процессы анализа данных.

Обучение бывает двух типов – «с учителем» (supervised) или «без учителя» (unsupervised). Первый тип подразумевает предварительную разметку данных, то есть каждый набор данных имеет пометку, например, «данные здорового человека»/«данные больного» или «нормальная финансовая операция»/«мошенническая операция» и т. п. Машина находит закономерности, по которым новые операции можно отнести к той или другой категории и дальше уже сама учится размечать новые. Такие алгоритмы позволяют, например, детектировать отклонения от нормы на ранней стадии – до начала болезни человека или до мошенничества, до поломки двигателя, до компьютерной атаки и т. п., что позволяет предсказывать опасные состояния анализируемой системы.

Второй тип обучения обходится без разметки и используется тогда, когда невозможно предварительно разметить данные ввиду отсутствия чётких критериев, недостатка данных или времени. Тогда хорошие состояния анализируемой системы определяются статистически, например, то, что укладывается в 90% похожих событий – это норма, а отклонения от неё – плохие состояния.

Большинство сегодняшних алгоритмов искусственного интеллекта используют оба метода в зависимости от того, какой более эффективен. В безопасности, например, метод обучения на размеченных данных часто называют методом чёрных списков, поскольку есть примеры плохих состояний (атак, вирусов, признаков мошенничества), которые не надо пропускать. Но такой метод позволяет бороться только с известными атаками и нарушениями, то есть только с теми, от каких уже кто-то пострадал, и признаки этих нарушений попали в базы данных атак или нарушений. Для того чтобы бороться с неизвестными атаками, а именно они наиболее опасны, применяется метод белых списков, то есть обучение на неразмеченных данных. В этом случае система искусственного интеллекта обращает внимание не на признаки нарушений, а на отклонения от обычного течения процесса.

– Как вы встраиваете свои продукты в эти тренды?

Любой часто повторяющийся процесс содержит некоторые закономерности, позволяющие разделять нормальное течение процесса и отклонения, а в нашей отрасли отклонения означают нарушения: кибератаки, мошенничество, вирусы, нарушение политик обращения с конфиденциальными данными, компьютерные сбои и другие состояния системы, опасные для инфраструктуры и данных. Поэтому сегодня практически каждый продукт информационной безопасности содержит в той или иной мере алгоритмы искусственного интеллекта.

Мы с самого начала ставили задачу работы наших продуктов активно и без участия человека – атаки и нарушения должны определяться и блокироваться. Засилье в информационной безопасности пассивных продуктов – то есть тех, которые лишь оповещали оператора об инциденте, но не блокировали его – было связано с большой долей ложных срабатываний, поэтому окончательное решение принимал человек. Блокировать легитимные процессы и останавливать этим бизнес – не лучший способ защиты, поэтому мы изначально сделали ставку на снижение доли ложных срабатываний до уровня меньшего, чем допускает оператор-человек. Используя технологии искусственного интеллекта, обучаясь на данных мониторинга трафика, имитируя действия оператора, получая данные от систем анализа защищённости и встраиваясь в защищаемые бизнес-процессы, мы снизили ложные срабатывания до 1-2%, что уже лучше, чем результаты живого оператора.

Такой подход позволил построить систему защиты, которая не требует живого оператора, а работает сама по принципу «включил и забыл». Система продолжает защищать процесс, даже если он постоянно меняет функциональность – для этого используются методы адаптивной безопасности: как только защищаемая система изменяется, робот-защитник исследует изменения, проверяет новую функциональность на уязвимости, а найдя – вносит изменения в программу защиты, не допуская злоумышленников к уязвимой функциональности. Таки образом удаётся без участия человека защищать системы, строящиеся по принципу эджайл (agile).

Спрос на такие системы выше там, где сложно найти и удержать специалистов в области мониторинга атак – небольшие компании, государственные услуги и регионы. Поэтому в нашем случае замена людей-операторов роботами – это не бесчеловечный технократический тренд, а ответ на критический дефицит специалистов в области информационной безопасности.

На вопросы отвечал Рустем Хайретдинов – вице-президент группы компаний Infowatch.

INFOWATCH®

***Infowatch** – разработка решений для защиты от внутренних и внешних угроз, а также информационных атак.*

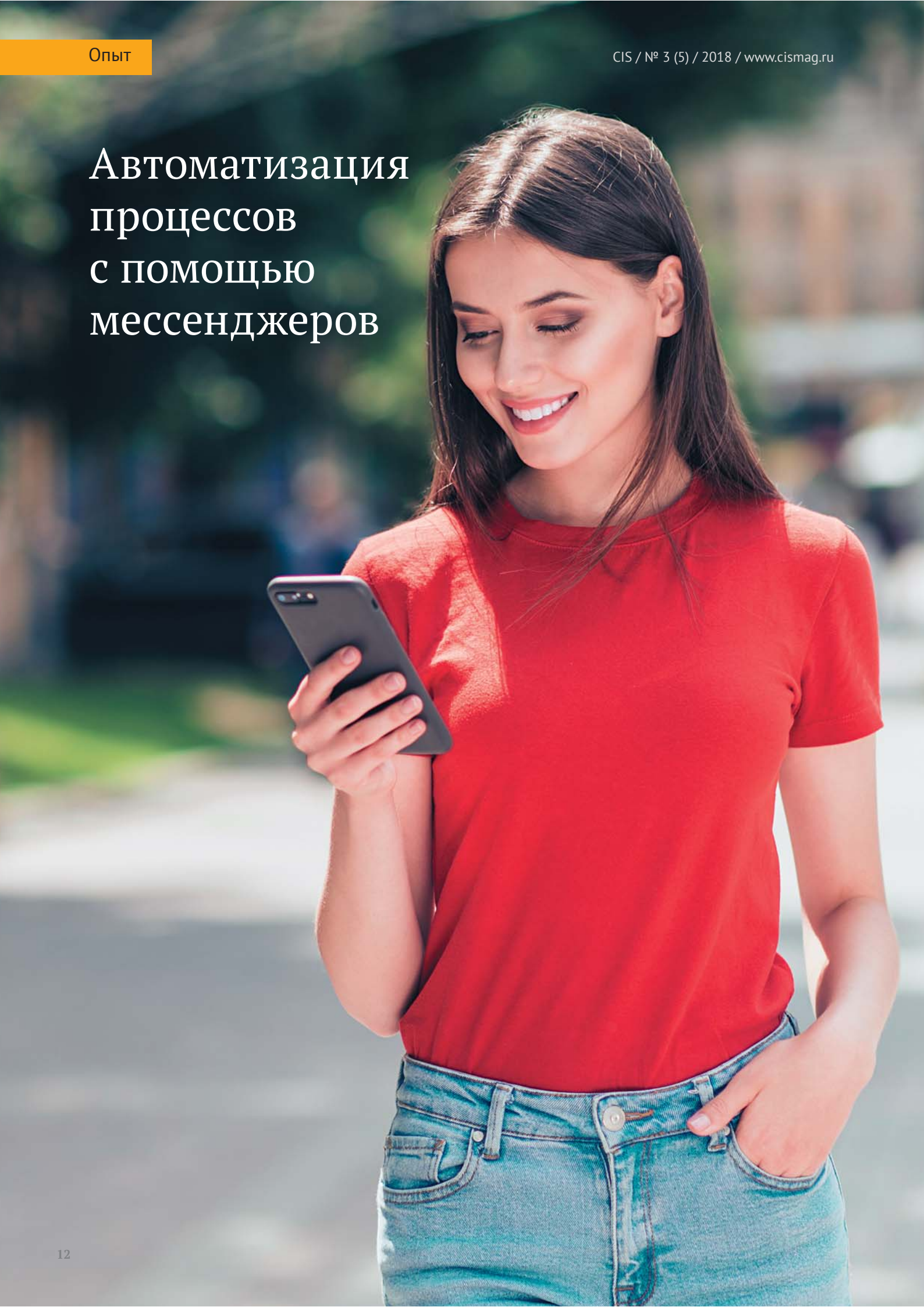
www.infowatch.ru

eToken

Продукты линейки eToken –
основа инфраструктуры информационной
безопасности современного предприятия

etokenstore.ru

Автоматизация процессов с помощью мессенджеров



Как всё начиналось

Так случилось, что ко мне обратились знакомые за помощью в автоматизации заказа пропусков. Задача была в том, чтобы сотрудники, которые работают зачастую не за компьютерами, могли оформлять заказ на пропуск на внешних гостей.

Идеи были разные:

- бумажные заявки отметались сразу же, так как территория большая и носить бумажки долго и вырывает людей из рабочего процесса;
- терминалы для заказов пропуска получались слишком дорогостоящими для подобной задачи и ни в каком виде не оправдывали вложений;
- приложение для телефона показалось хорошим решением, но встала необходимость разработки под различные платформы, что увеличивало трудозатраты на разработку;
- самой успешной идеей оказалась использование уже готовой платформы в виде обычного мессенджера.

Так как доблестными стараниями РКН Telegram работает не совсем стабильно на территории РФ, у WhatsApp отсутствует требуемая функциональность для написания более или менее функциональных чат-ботов, то выбор остановили на Viber.

Автоматизация процесса

Процесс заказа пропуска довольно-таки прост: несколько вопросов о госте, таких как ФИО, информация по машине и дата посещения. Затем по полученной информации формируется файл Microsoft Excel и почтой отправляется дальше на обработку в отдел пропусков.

Таким образом, сотрудник, находясь в любом месте, вдали от компьютера, может заказать пропуск для гостя.

В итоге получили удобный инструмент для сотрудников, которые заказывают пропуск своим гостям, так как телефон всегда с собой и нет необходимости срочно бежать к компьютеру или звонить и диктовать данные. С другой стороны, служба, занимающаяся пропусками, получает все заявки в строго определённом формате, их остаётся только распечатать и выдать посетителям.

Несколько слов о реализации

Итак, первым делом идём в партнёрский раздел и регистрируем «паблик аккаунт» (публичная учётная запись). После регистрации получаем некий токен (набор символов), по которому нашего чат-бота будет идентифицировать сервер Viber. Регистрация вполне простая и вопросов не вызывает.

Далее мы регистрируем наш сценарий, куда будут перенаправляться все события, на которые должен наш чат бот реагировать, и приступаем к разработке.

API (программный интерфейс) Viber описывать не буду, так как всё хорошо описано в официальной документации. Скажу только, что по сравнению с API Telegram, этот интерфейс не очень функциональный и какой-то слишком простоватый.

После того как пользователь подключился к чат-боту, он переходит в режим ожидания активации. Это необходимо, чтобы можно было контролировать, кто имеет право отправлять заявки на заказ пропуска. Администратор через чат-бота имеет возможность просмотреть в административном интерфейсе всех пользователей, подключившихся к чат-боту, и активировать тех из них, которым необходимо предоставить функциональность заказа пропусков. При этом стоит отметить, что при подключении на сервер с Viber-клиента передаётся имя пользователя для идентификации администратором.

После того как администратор активирует пользователя, пользователь получает возможность осуществлять заказ пропусков.

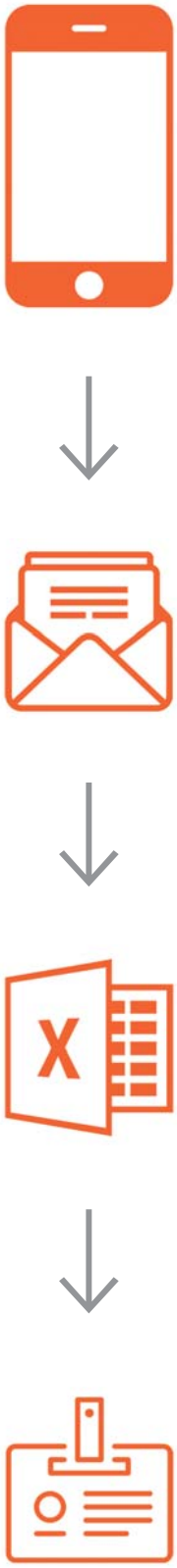
Как уже упоминалось ранее, у чат-бота есть административный интерфейс, в котором можно управлять администраторами (теми, кто имеет доступ к этому административному интерфейсу), пользователями (удалять и активировать/деактивировать их), просматривать и выгружать события журнала.

Ведение журнала событий чат-бота позволяет отслеживать, кем, для кого и когда были заказаны пропуска, также осуществляется ведение журнала работы самого чат-бота, что позволяет выявлять ошибки или перебои в работе.

Данное решение может применяться для автоматизации процесса заказа пропусков арендаторами в больших бизнес-центрах или складских терминалах. При этом сведения о компании и арендаторе, указанные в пропуске, будут зависеть от того, сотрудник какой организации заказал пропуск.

Вместо эпилога

Мессенджеры могут быть использованы не только для общения, но и как простая, но удобная и универсальная платформа для автоматизации бизнес-процессов.



СОВИНТЕГРА

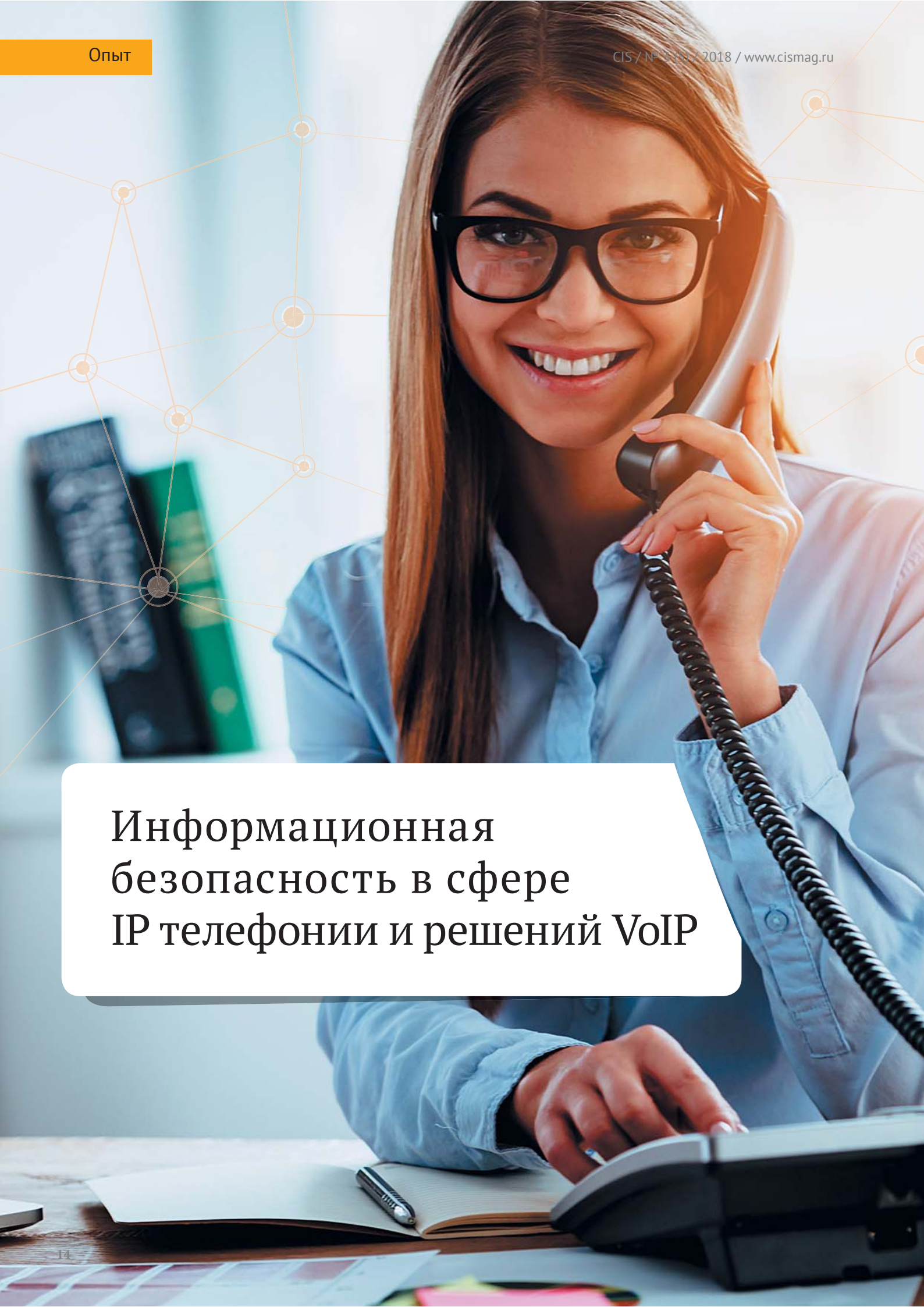
«СОВИНТЕГРА»

Наша основная специализация – защита ценных информационных активов и полный спектр ИТ-услуг и решений.

+7 (499) 136-27-31

info@sovintegra.ru

www.sovintegra.ru



Информационная безопасность в сфере IP телефонии и решений VoIP

На сегодняшний день проблемы информационной безопасности в мире приобретают всё большую актуальность. В СМИ часто можно наткнуться на новость об очередной успешной хакерской атаке, крупной утечке критичных данных или очередном вирусе-вымогателе, который срывает работу целых компаний.

Даже если вы человек далёкий от информационной безопасности и мира информационных технологий, то вы всё равно наверняка слышали о вирусе WannaCry, уязвимостях Spectre и Meltdown и, может быть, даже о недавней атаке на устройства компании Cisco, которая ударила по крупным провайдерам и парализовала много сервисов и сетевых сегментов.

Однако широкой огласке обычно подвергаются новости об атаках и уязвимостях, носящих массовый характер и направленных на наиболее распространённые инфраструктурные системы. Мы же хотим рассказать о том, как обстоит ситуация с информационной безопасностью в отдельной в отдельно взятой сфере – IP-телефонии и решений VoIP. Разберём наиболее важные проблемы и тренды развития данного направления.

Проблемы информационной безопасности в VoIP

Если раньше, выбирая на чём строить офисную телефонию, заказчиков больше всего волновали вопросы стоимости и надёжности, то в связи с нынешним положением, вопросы защиты и безопасности всё чаще начинают преобладать. Хотя IP-телефония имеет массу преимуществ по сравнению с системами традиционной телефонии, её намного легче взломать. В случае с традиционной системой PSTN злоумышленник должен получить физический доступ к среде передачи или системам, которые задействованы в обмене голосовой информацией. IP-телефония – это прежде всего сеть с коммутацией пакетов, которые передаются наряду с другими корпоративными сервисами – интернетом, почтой и др. Если эта сеть недостаточно защищена, то злоумышленнику даже не обязательно находиться в одной стране с системой IP-телефонии, чтобы получить доступ к критичным данным, украсть их или модифицировать.

Вот почему необходимо обеспечивать многоуровневую защиту систем корпоративной IP-телефонии. Недостаточно просто поставить стойкий пароль к интерфейсу управления. Это должен быть чёткий набор определённых мер, применяемых в комплексе: межсетевое экранирование, антивирусная защита, регулярные обновления программного обеспечения, шифрование передаваемых данных и другое.

Отдельно следует уделить внимание повышению осведомлённости своих сотрудников об атаках из разряда социальной инженерии. Одним из наиболее распространённых векторов атаки данного типа на сегодняшний день является фишинг. Суть его заключается в том, что злоумышленник рассылает «письма счастья» с вредоносными вложениями в надежде на то, что человек откроет это вложение и тем самым загрузит на свой компьютер вредоносное ПО. Защититься от таких атак можно сразу на нескольких уровнях.

1. Межсетевой экран, на котором адрес отправителя фишинговых писем должен быть заблокирован. Автоматизировать процесс получения актуального списка адресов активных отправителей для блокировки на МСЭ можно с помощью решений Threat Intelligence. Существуют как платные решения от таких компаний, как Anomali, ThreatConnect или EclecticIQ, так и решения с открытым исходным кодом, например, YETI и MISP.

2. Решение для защиты почтового сервера, которое проверяет все письма на предмет подозрительных вложений, адреса отправителя, блокирует спам. Примерами таких решений являются Kaspersky Security для почтовых серверов, AVG Email Server Edition для ME, McAfee Security for Email Servers. Кстати, в этом случае также можно автоматизировать процесс блокировки с помощью решений TI.

3. Антивирусное ПО для защиты оконечных устройств, которое заблокирует опасное вложение, если всё-таки вредоносное ПО сможет пролезть через МСЭ и почтовый сервер. Для этого подойдёт Kaspersky Endpoint Security, Norton, Trend Micro и другие.

Но если от фишинга можно защититься с помощью специализированных программ и аппаратных решений, то от следующих видов атак, основанных на социальной инженерии, защититься гораздо труднее. Возможно, вы не знали, но помимо традиционного email-фишинга, существует также и телефонный. Например, сотруднику вашей компании на голосовую почту может прийти сообщение от «банка» о том, что кто-то пытался получить доступ к его счёту и что ему необходимо срочно перезвонить по оставленному номеру. Нетрудно догадаться, что на другом конце провода его будет ждать злоумышленник, который постарается сделать всё, чтобы втереться в доверие, украсть данные его счёта, чтобы в итоге похитить денежные средства.

Существует также телефонный вишинг. Этот тип атаки направлен на первую линию сотрудников, которые принимают все входящие звонки в вашей компании. На общий номер поступает звонок от какой-нибудь известной организации или персоны, а дальше с помощью методов психологического давления доверчивого сотрудника заставляют что-либо сделать. В самом лучшем случае позвонивший будет агрессивно требовать соединить его с руководством компании, чтобы предложить какие-нибудь услуги, в самом худшем – выдать конфиденциальную или критически важную информацию. А что если злоумышленник узнает каким банком обслуживается ваша компания и позвонит бухгалтеру от лица «вашего банка?» К такому тоже нужно быть готовым.

Защититься от подобного типа атак можно было бы с помощью некоего аналога Threat Intelligence для VoIP – списка телефонных номеров, с которых поступают фишинговые и вишинговые звонки, чтобы заблокировать их на АТС. Однако такого решения пока нет, поэтому придётся просвещать сотрудников на тему безопасности.

Безопасность «облачных» систем

Сейчас уже сложно обозначить чёткие границы офисной сети. С распространением «облачных» решений, распределённых сетей VPN и всеобщей виртуализации корпоративная сеть уже перестала иметь чёткую географическую привязку.

Аналогично обстоят дела и в сфере VoIP. Каждый крупный провайдер IP-телефонии имеет в своём наборе услуг «облачную» АТС, которая настраивается в считанные минуты и способна обеспечить телефонией компанию любого размера, неважно где территориально эта компания расположена. «Облачная» или виртуальная АТС – это очень удобное решение, которое привлекает заказчиков тем, что не надо держать лишние серверы в здании и обслуживать их. Вместо этого можно просто арендовать необходимые серверные мощности или сервис телефонии. Однако с точки зрения информационной безопасности «облачные» АТС – это идеальная цель для хакерских атак. Потому что, как правило, учётные записи для доступа к настройкам АТС находятся в открытом доступе. Если владелец учётной записи не озаботится созданием стойкого пароля, то он рискует оплатить немаленький счёт за телефонные разговоры злоумышленника или предоставить доступ к записям разговоров своих сотрудников. В этой связи при выборе провайдера следует также проверить, обеспечивает ли он дополнительные мероприятия по защите целостности и конфиденциальности данных. Используется шифрование при подключении к учётной записи с настройками «облачной» АТС, шифруются ли данные при их транспортировке.

Тренды развития направления ИБ в VoIP

Наиболее распространённым методом защиты корпоративной инфраструктуры является организация защищённой сети VPN, когда подключение извне осуществляется по зашифрованному каналу, а данные внутри сети передаются в незашифрованном виде. Это относится и к голосовому трафику. Однако тенденции развития информационных технологий указывают на то, что в недалёком будущем голосовая информация также будет подвергаться шифрованию. Большинство VoIP-вендоров уже давно имплементируют в своих решениях поддержку таких протоколов, как SIP/TLS, SRTP, ZRTP и др., стимулируя пользователей внедрять ещё один уровень защиты. Например, большинство IP-телефонов и решений видеоконференцсвязи от компании Cisco, а также системы CUCM, CUBE, Cisco SBC, UCCS и др. поддерживают TLS 1.2 и SRTP. Самое распространённое решение с открытым исходным кодом, IP-АТС Asterisk, имеет поддержку защищённых протоколов передачи медиатрафика начиная с версии 1.8. В программной АТС 3CX версии V15 на базе Windows поддержка SRTP включена по умолчанию.

VoIP-решения зачастую очень тесно интегрируются с другими корпоративными системами, такими как CRM, ERP, CMS, не говоря уже о таких каналах бизнес-коммуникаций, как email, обмен мгновенными сообщениями (чат) и социальные сети, формируя в совокупности концепцию UC (Unified Communications). Потенциальные преимущества, которые несёт данная концепция, очень привлекательны, но вместе с тем создаётся множество точек, уязвимых к возможному взлому. Недостаточный уровень защиты одной из них может быть угрозой всей корпоративной сети. Поэтому разработчики, несомненно, будут усиливать безопасность каналов интеграции данных систем.

Можно также ожидать интеграцию систем корпоративной телефонии в такие средства защиты, как DLP (средства защиты от утечек), адаптации метрик VoIP в SIEM-системах (система управления информацией и событиями безопасности), а также появление унифицированных репутационных баз (Threat Intelligence) со списками потенциально опасных номеров или других индикаторов компрометации, относящихся к VoIP, которые будут автоматически блокироваться имеющимися средствами защиты.

MERION NETWORKS

Мерион Нетворкс

Внедрение качественных и доступных ИТ-решений, направленных на повышение эффективности бизнес процессов.

www.merionet.ru

Astra Linux Special Edition релиз Смоленск 1.6

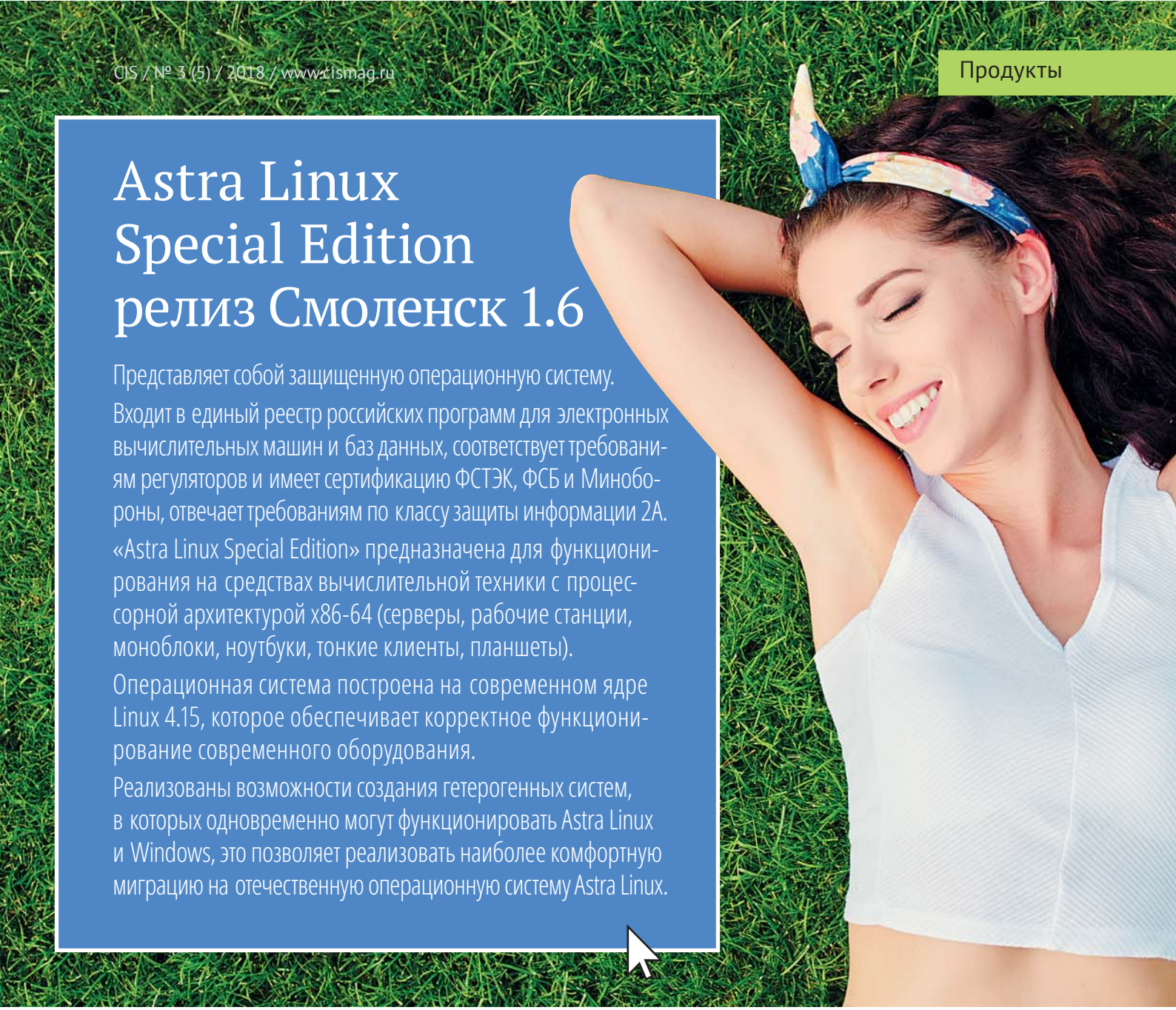
Представляет собой защищенную операционную систему.

Входит в единый реестр российских программ для электронных вычислительных машин и баз данных, соответствует требованиям регуляторов и имеет сертификацию ФСТЭК, ФСБ и Минобороны, отвечает требованиям по классу защиты информации 2А.

«Astra Linux Special Edition» предназначена для функционирования на средствах вычислительной техники с процессорной архитектурой x86-64 (серверы, рабочие станции, моноблоки, ноутбуки, тонкие клиенты, планшеты).

Операционная система построена на современном ядре Linux 4.15, которое обеспечивает корректное функционирование современного оборудования.

Реализованы возможности создания гетерогенных систем, в которых одновременно могут функционировать Astra Linux и Windows, это позволяет реализовать наиболее комфортную миграцию на отечественную операционную систему Astra Linux.



Astra Linux – единая платформа и интерфейс для всех видов и типов устройств, совместимая со многими передовыми платформами: X86_64, MIPS, ARM, PowerPC, IBM System Z.

Более 1000000 пользователей ежедневно решают свои рабочие задачи на отечественной операционной системе Astra Linux. Стать флагманом процесса импортозамещения в сфере отечественного программного обеспечения Astra Linux смогла благодаря простой навигации, стабильной работе и современному пакету программ.

Пользователи операционных систем Astra Linux могут быть уверены в защищённости конфиденциальной информации, а также получают долгосрочную техническую поддержку в вопросах установки и настройки операционной системы. Кроме того, переход на ОС Astra Linux экономически выгоден: происходит снижение затрат на рабочие станции и серверы. В качестве примера приведены исходные данные 100 рабочих станций и 10 серверов.

Рабочая станция	**Сервер**	**Рабочая станция**	**Сервер**
ОС Windows 10 Enterprise		ОС AstraLinux Special Edition (OEM) (BOX]	
11 799 ₽	–	–	14 900 ₽
ОС Windows Server 2016		Дополнительный комплект	
1 347 ₽	47 432 ₽	13 900 ₽	13 900 ₽
СУБД Microsoft SQL Server		СУБД PostgreSQL	
9 630 ₽	41 378 ₽	–	Входит в ОС
Exchange Server 2013 Standard		Почтовые сервера Dovecot	
4 047 ₽	32 636 ₽	–	Входит в ОС
Microsoft Office 2016 Std		LibreOffice	
13 647 ₽	–	Входит в ОС	–
Стоимость одной ЭВМ			
40 470 ₽	121 446 ₽	13 900 ₽	14 900 ₽
Совокупная стоимость для АС			
4 047 400 ₽	1 214 460 ₽	1 390 000 ₽	150 000 ₽
5 261 460 ₽		**1 540 000 ₽**	

Партнёры аппаратного обеспечения

HUAWEI, IBM, DELL, hp, DEPO [computers], AQUARIUS, ICL, acer, Canon, kraftway, TONK, SAMSUNG, iru, РАМЭК, Lenovo

Партнёры программного обеспечения

1С, infotecs, Аладдин рд, КОДЕКС, ISBC, Компания АКТИВ, KASPERSKY, SAP, СИГМА, МойОфис, КонсультантПлюс, LibreOffice, КРИПТОПРО, Postgres PROFESSIONAL

Разработчик Astra Linux АО «НПО РусБИТех», ведёт активную программу поддержки производителей оборудования и программного обеспечения READY FOR ASTRA LINUX. Целью программы является создание преимущественного положения на отечественном рынке информационных технологий производителей программного и аппаратного обеспечения за счёт информирования потребителей о совместимости с отечественной защищённой операционной системой в Российской Федерации.

Сотрудниками АО «НПО РусБИТех» разработана программа обучения для пользователей с различным уровнем подготовки. Курсы будут полезны как опытным системным администраторам, так и начинающим пользователям. Широкая сеть обучающих центров позволит с комфортом провести обучение в удобном для вас регионе.

Существуют условия лицензирования операционной системы общего назначения Astra Linux Common Edition для государственных учебных заведений. Для создания учебных классов осуществляется безвозмездная передача неисключительного права на операционную систему. Службой технической поддержки оказывается содействие в вопросах установки и настройки операционной системы. Основная цель – подготовка будущих специалистов для работы на отечественной операционной системе.

Не так давно компания представила на рынке новую версию операционной системы общего назначения Astra Linux Common Edition релиз «Орёл» версия 2.12.

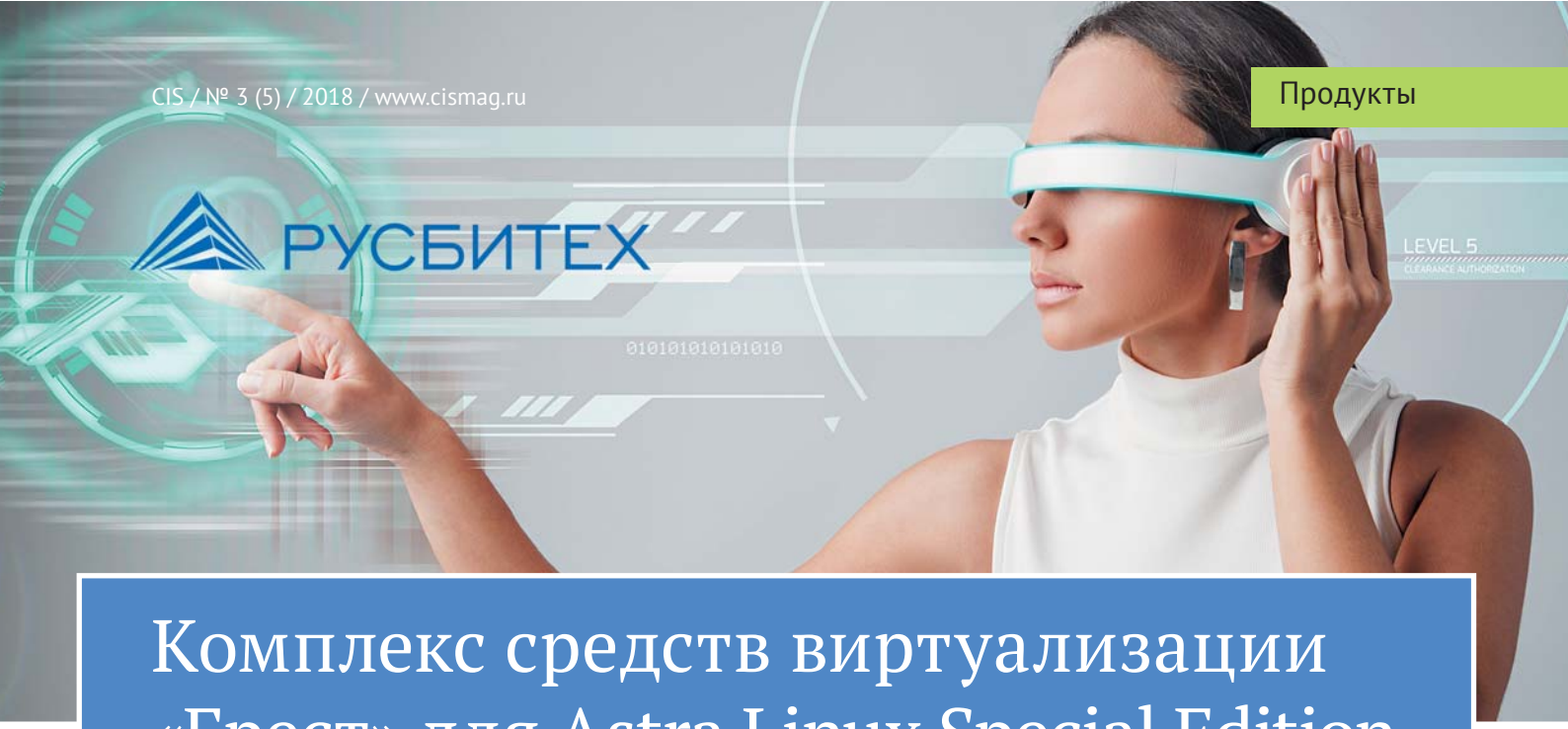
Основные изменения коснулись пользовательского интерфейса. Обновлён графический интерфейс. Теперь он выполнен в плоском стиле – в соответствии с современными тенденциями. Добавлено новое оформление рабочего стола с возможностью выбора пользовательской цветовой палитры. Доработаны программы для работы с мультимедийными и гипертекстовыми материалами для мобильного режима интерфейса пользователя. Обновлены офисные приложения.

Кроме этого, в состав операционной системы общего назначения включено современное ядро Linux 4.15, обеспечивающее корректное функционирование современного оборудования.

НАУЧНО-ПРОИЗВОДСТВЕННОЕ ОБЪЕДИНЕНИЕ РУСБИТЕХ

АО «НПО РусБИТех»
Акционерное общество «Научно-производственное объединение Русские базовые информационные технологии»

www.rusbitech.ru | mail@rusbitech.ru



Комплекс средств виртуализации «Брест» для Astra Linux Special Edition

Комплекс средств виртуализации «Брест» предназначен для создания защищённой виртуальной среды, обеспечивающей функционирование виртуальных машин и управление ими в операционной системе Astra Linux Special Edition в условиях дискреционного и мандатного разграничения доступа. В настоящий момент не существует аналогов комплекса, который бы в совокупности имел тот же состав, функциональные возможности, оптимальность конфигурации, надёжность защиты, высокую производительность, стабильность работы, простоту установки и частоту обновлений.

Входящие в состав комплекса компоненты (СУБД, средства электронной почты, веб-технологии, офисные средства, виртуализация и др.) позволяют применять его как в составе автономных ЭВМ, так и территориально-распределённых автоматизированных систем любой сложности.

Ниже представлены программные возможности.

- Централизованное управление одним или несколькими ЦОД.
- Централизованное управление кластером (или несколькими кластерами), входящими в ЦОД.
- Централизованное управление хостом (сервером) в каждом кластере. Поддерживаются серверы архитектуры Intel x86_64 с конфигурацией до 160 логических процессоров, имеющих до 2 ТБ ОЗУ каждый. Для процессоров должны быть доступны технологии виртуализации.
- Централизованное управление пулом виртуальных машин (ВМ). Поддерживаются виртуальные машины Intel x86_64 или Intel x86 с конфигурацией до 64 виртуальных процессоров и до 2 ТБ ОЗУ каждая.
- Централизованное управление пользователями, интеграция с доменами ALD.
- Идентификация, аутентификация и авторизация пользователей, операторов и обслуживающего персонала для получения сеанса работы с рабочим столом ВМ через домен безопасности.
- Мандатная, дискреционная и ролевая модели разграничения доступа субъектов (пользователей) к объектам (виртуальные машины, хосты, кластеры, ЦОД и др.). Контроль целостности.
- Централизованный аудит.
- Формирование отчётов.
- «Живая» миграция виртуальных машин.
- Создание кластеров высокой доступности (High Avaliability).
- Построение политик по распределению нагрузки.
- Мониторинг аппаратного состояния серверов, входящих в ЦОД. Поддерживается работа с низкоуровневыми интерфейсами управления аппаратной платформой (ILO, IPMI и т.п.).
- Проброс USB-устройств в обе стороны (как на клиента, так и от него), разграничение доступа к этим устройствам.
- Поддержка современных операционных систем Linux и Windows в качестве гостевых операционных систем.
- Использование клиентских рабочих мест под управлением как Linux, так и Windows.
- Минимальные требования к рабочему месту оператора – браузер.
- Получение сеанса работы с виртуальной машиной по протоколу VNC или SPICE. В случае использования протокола SPICE обеспечивается работа со звуком и USB-устройствами.
- Поддержка агрегации (логического объединения портов) сетевых соединений при построении высокопроизводительной отказоустойчивой сетевой инфраструктуры.
- Создание нескольких сетей и разделение служебного и пользовательского трафика на разные информационные потоки, поддержка VLAN.
- Поддержка распределённого хранилища Ceph в качестве подключаемого хранилища.
- Поддержка ФС NFS, CIFS, стандарта iSCSI или ФС сервера (хоста) в качестве хранилища.
- Установка драйверов паравиртуализации в гостевые операционные системы.

CIS / № 3 (5) / 2018 / www.cismag.ru

Продукты компании «Аладдин Р. Д.» для перехода на новые ГОСТ

В соответствии с выпиской из документа ФСБ России № 149/7/1/3-58 от 31.01.2014 «О порядке перехода к использованию новых стандартов ЭЦП и функции хэширования» использование схемы подписи ГОСТ Р 34.10-2001 для формирования подписи **после 31 декабря 2018 года не допускается.** На момент написания данного материала дополнительных сведений от регуляторов не поступало.

Клиентам, использующим устройства JaCarta ГОСТ и eToken ГОСТ, необходимо завершить переход на новые ГОСТ как минимум **на месяц раньше**, так как сертификат соответствия ФСБ России № СФ/111-2750 на персональное средство ЭП «Криптотокен ЭП» (по ГОСТ Р 34.10-2001) в составе изделий JaCarta ГОСТ и eToken ГОСТ действует **до 1 декабря 2018 г. и продлеваться не будет.**

Ниже представлена таблица продуктов компании «Аладдин Р. Д.», которые помогут вовремя перейти на ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012:

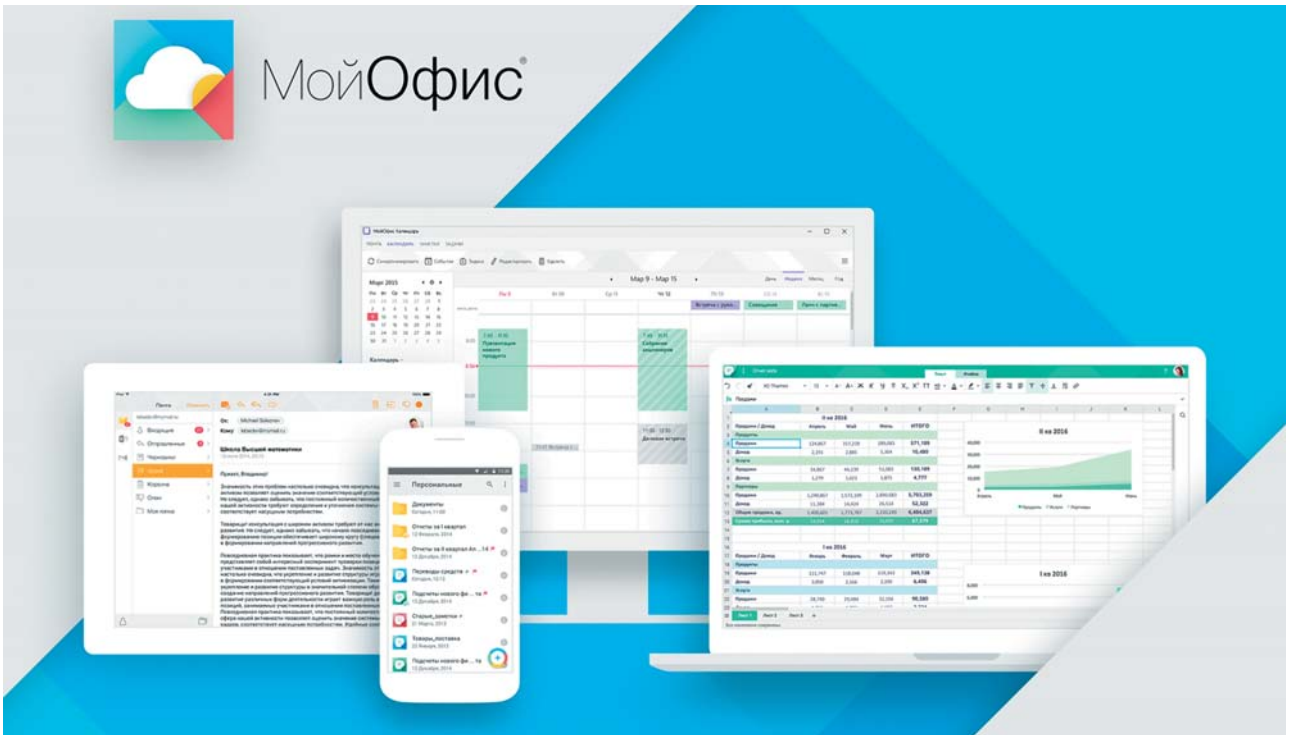
Старые ГОСТ	Новые ГОСТ	Описание
• eToken ГОСТ • JaCarta ГОСТ	JaCarta-2 ГОСТ	USB-токены, смарт-карты и модули безопасности (SIM, чипы для монтажа на печатную плату) для строгой аутентификации и работы с усиленной квалифицированной ЭП, аппаратно поддерживающие как новые криптоалгоритмы ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2012, так и старые – ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 и ГОСТ 28147-89. Сертификаты: • ФСБ России – на средство криптографической защиты информации (СКЗИ) класса КС1 и КС2, а также как средство ЭП класса КС1 и КС2; • ФСТЭК России – может применяться в АИС до класса защищённости 1Г, в ГИС до 1 класса защищённости, в ИСПДн до 1 уровня защищённости.
• JC-WebClient 3.0 и ниже	**JC-WebClient 4.0 и выше**	Решение для реализации функций строгой двухфакторной аутентификации, работы с ЭП и шифрования данных в веб-приложениях и «облачных» сервисах с использованием USB-токенов и смарт-карт семейства JaCarta, в том числе JaCarta-2 ГОСТ. Включено в единый реестр отечественного ПО.

• JaCarta SE	**JaCarta-2 SE**	USB-токены для работы в специализированных информационных системах, в том числе в единой государственной автоматизированной информационной системы учёта объёма производства и оборота этилового спирта, алкогольной и спиртсодержащей продукции (ЕГАИС). Поддерживаются как новые криптоалгоритмы ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2012, так и старые – ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 и ГОСТ 28147-89. Сертификаты: • ФСБ России – на средство криптографической защиты информации (СКЗИ) класса КС1 и КС2, а также как средство ЭП класса КС1 и КС2; • ФСТЭК России – может применяться в АИС до класса защищённости 1Г, в ГИС до 1 класса защищённости, в ИСПДн до 1 уровня защищённости.
• JaCarta ГОСТ – управление и администрирование • Единый Клиент версии JaCarta 2.9 и ниже	**Единый Клиент JaCarta 2.11 и выше**	Клиентское ПО, обеспечивающее возможность работы с устройствами семейства JaCarta, в том числе JaCarta-2 ГОСТ. Включено в единый реестр отечественного ПО. Сертификаты: • ФСТЭК России – может применяться в АИС до класса защищённости 1Г, в ГИС до 1 класса защищённости, в ИСПДн до 1 уровня защищённости.
• JaCarta Management System (JMS) 3.1.1 и ниже	JaCarta Management System (JMS) 3.3 и выше	Корпоративная система управления жизненным циклом USB-токенов и смарт-карт, поддерживающая устройства различных производителей, в том числе JaCarta-2 ГОСТ. Включена в единый реестр отечественного ПО. Сертификаты: • ФСТЭК России – может применяться в АИС до класса защищённости 1Г, в ГИС до 1 класса защищённости, в ИСПДн до 1 уровня защищённости.

Знакомство с продуктами МойОфис

Мир корпоративной информационной среды уже не будет прежним. В том числе потому, что всё большее место в информационном ландшафте предприятий занимают российские разработки.

До 90 % рабочего времени и до 30 % жизни занимает взаимодействие человека с программными приложениями. Мы редактируем документы различного формата, реализуем проекты совместно с коллегами и создаём презентации для клиентов, составляем график деловых встреч и общаемся по электронной почте. Всё это – повседневные офисные задачи.



Требования современных пользователей постоянно растут, и рынку становятся необходимы офисные приложения нового поколения, отличающиеся лёгкостью интерфейса и удобством использования. Всё больше государственных организаций, коммерческих предприятий и образовательных учреждений используют для решения своих повседневных офисных задач отечественный продукт «МойОфис».

«МойОфис» в офисе без границ

«МойОфис» – это набор офисных приложений для работы с документами и корпоративный почтовый сервер. С использованием инструментов «МойОфис» легко решать ежедневные рабочие задачи – как на компьютерах, так и на мобильных устройствах из любой точки мира.

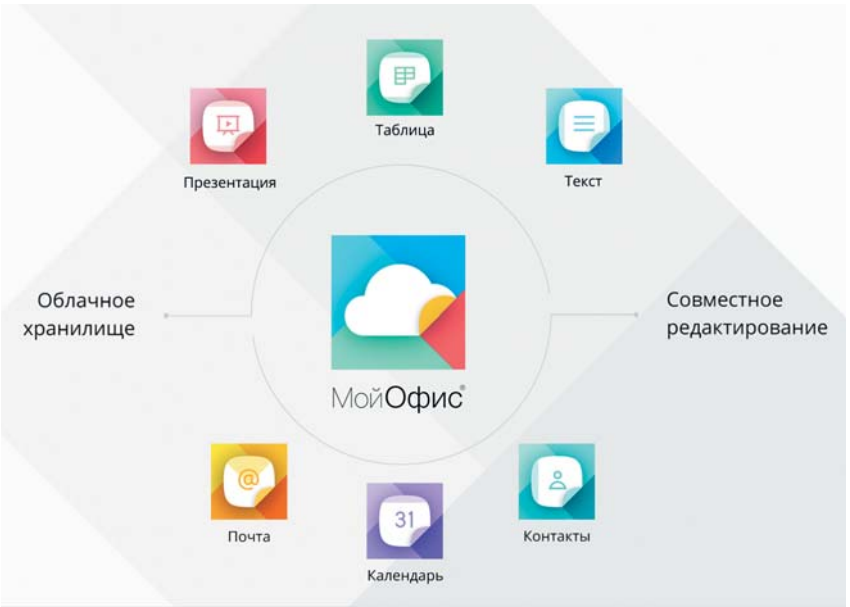
Какие рабочие процессы обеспечивает «МойОфис»? В первую очередь это работа с текстами и электронными таблицами с возможностью совместного редактирования, настройкой прав доступа и сохранения истории изменений документов. Инструменты «МойОфис» позволяют создавать презентации и быстро просматривать доклады. Совместная работа реализована через корпоративный мессенджер с поддержкой аудио- и видеоконференций. Есть и привычные, но не менее важные функции управления почтой, календарём и контактами. Сотрудник полноценно участвует в рабочих процессах, находясь за пределами офиса и имея доступ к корпоративным документам, ресурсам и приложениям на своём планшете или смартфоне.

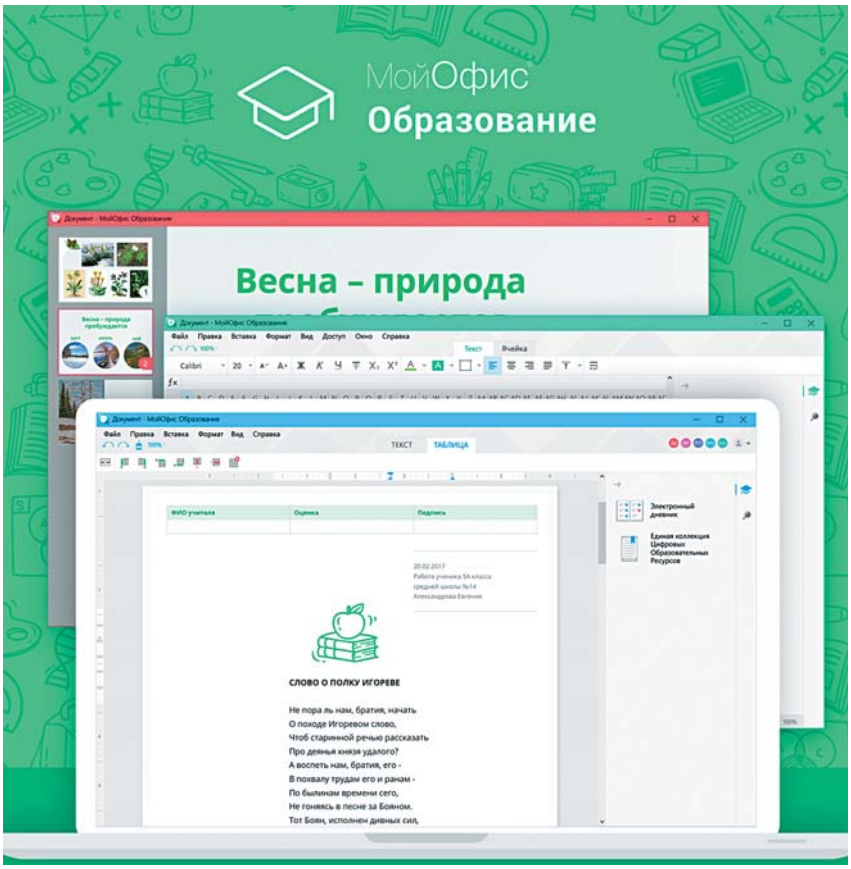
Редакторы «МойОфис» совместимы с открытыми форматами документов, в том числе.odx,.ods,.odp (ГОСТ Р ИСО/МЭК 26300-2010), и с более популярными проприетарными —.doc/.docx,.xls/.xlsx,.ppt/.pptx.

Интерфейсы «МойОфис» отвечают современным тенденциям: они просты для восприятия, удобны в работе с различными документами и электронной корреспонденцией.

Разработанное в России, программное обеспечение «МойОфис» отвечает новым стандартам и актуальным трендам в безопасности работы с документами. Все пакеты приложений внесены в реестр отечественного ПО и могут быть использованы в соответствии с программой импортозамещения на российском ИТ-рынке.

Компания «Новые облачные технологии» представила рынку продуктовую линейку «МойОфис» в 2015 году.





Сегодня разработчик предлагает пять пакетов приложений «МойОфис»:

- «МойОфис Профессиональный»;
- «МойОфис Стандартный»;
- «МойОфис Частное облако»;
- «МойОфис Почта»;
- «МойОфис Образование».

«МойОфис Профессиональный», «Стандартный», «Частное облако»: преимущества в отличиях

«МойОфис Профессиональный» – это 13 сервисов для создания корпоративной информационной среды в государственных учреждениях, корпорациях и коммерческих предприятиях. В его состав входят основные офисные редакторы и инструменты организации рабочего процесса. Среди приложений: «МойОфис Текст», «МойОфис Таблица», «МойОфис Презентация» и редактор презентаций, «МойОфис Почта», «МойОфис Календарь», «МойОфис Контакты» и «МойОфис Хранилище».

Отличительная особенность продукта – возможность онлайн-коммуникаций сотрудников и командной работы с файлами в единой системе, где бы вы ни находились. Для этого в пакет включены инструмент совместной работы «МойОфис Логос» и файловый менеджер «МойОфис Документы».

Более лаконичный набор сервисов предусмотрен в продукте «МойОфис Стандартный» – в него входят все настольные приложения профессионального пакета. «МойОфис Стандартный» разработан под операционные системы Windows и Linux. Он устанавливается на компьютерах пользователей и не требует подключения к интернету.

Организовать виртуальную рабочую среду поможет продукт «МойОфис Частное облако». С его помощью можно удалённо работать с документами в закрытом «облаке» в любых браузерах. Пакет «МойОфис Частное облако» поддерживает все те же рабочие процессы, что и «МойОфис Профессиональный». И, конечно, поддерживает политики защищённого корпоративного пространства для работы с данными и контроля доступа к ним.

«МойОфис Образование»: лицензии для школ и колледжей с нулевой стоимостью

Набор приложений для работы с текстами, презентациями и таблицами, который подходит как для обучения детей, так и для административной работы, – поставляется в пакете «МойОфис Образование». В соответствии с требованиями Федеральных государственных образовательных стандартов (ФГОС), редакторы «МойОфис Образование» дополнены специальной панелью «Образование». Эта консоль открывает быстрый доступ к популярным образовательным ресурсам напрямую из приложений. Интерфейс панели «Образование» можно настраивать с учётом специфики и географического положения каждого конкретного учебного заведения.

Но самое главное: число пользователей не ограничено и стоимость лицензий для детских садов, школ и колледжей – нулевая!

Экосистема «МойОфис» для коммуникаций – как это работает

Три приложения – «МойОфис»: «Почта», «Календарь» и «Контакты» – взаимосвязаны и совместимы со службами каталогов. Администратор может управлять учётными записями, группами и политиками. Сотрудникам удобно и просто пользоваться почтой, онлайн-календарём и быстро связываться с нужными людьми.

Мобильный «МойОфис» – бесплатно, скачиваем и тестируем

Чтобы офис был всегда под рукой, используйте мобильные приложения «МойОфис Документы» и «МойОфис Почта». Они адаптированы под мобильные платформы iOS и Android. Бесплатно скачать и протестировать мобильный «МойОфис» можно уже сейчас – он доступен в онлайн-магазинах App Store и Google Play.

Сегодня границы рабочего пространства стираются, а инструменты «МойОфис» доступны всегда и повсюду. Теперь вы знаете, как легко можно решать ёмкие задачи в любой компании, в любом уголке мира, на различных устройствах.

МойОфис

«Новые облачные технологии» – российская компания-разработчик полнофункционального офисного ПО для настольных ПК и мобильных устройств.

www.myoffice.ru

Российская платформа Docsvision для управления документами и информационными ресурсами компании

Владимир Андреев
президент компании, отвечает за продуктовую стратегию и развитие Docsvision

Компания «ДоксВижн» – создатель и разработчик системы управления документами и бизнес-процессами Docsvision. Система занимает 2-е место по популярности на рынке СЭД/ECM в России.

Среди клиентов – 1500 коммерческих предприятий и государственных организаций в России и странах ближнего зарубежья, в том числе Министерство экономического развития РФ, предприятия «Роснефти», компания «АЛРОСА», Администрация Екатеринбурга, энергетические компании, торговые сети и пр. Масштабы внедрений Docsvision – от десятков до десятков тысяч пользователей, от тысяч до миллионов документов, и в общей сложности сегодня с системой работают более 700000 пользователей.

2 место рейтинга «Самые популярные российские СЭД» (Tadviser, 2017)

2 место в исследовании «В поисках идеальной СЭД» (2017 г., GlobalCIO)

ТОП-3 рейтинга «Лучшие Workflow-движки в российских СЭД» (TAdviser, 2017)

3 место в рейтинге «BPM-системы-2018» (обзор российского рынка на TAdviser)

Залог множества успешных проектов и присутствия Docsvision в самых уважаемых рейтингах отрасли – это современный развивающийся продукт и грамотная бизнес-стратегия, принятая компанией на заре её становления.

20-летняя экспертиза в вопросах автоматизации

Сегодня в ДоксВижн» около 100 сотрудников, главный офис в Санкт-Петербурге. Первый прототип продукта появился в 1998 году под руководством Владимира Андреева. В 2005 году официально создаётся компания «ДоксВижн» – и уже через пару лет система уверенно закрепляется в тройке самых продаваемых российских СЭД. Сегодня Владимир Андреев и топ-менеджеры компании входят в состав ведущих отраслевых экспертных советов и принимают участие в формировании стандартов электронного документооборота, в т.ч. на государственном уровне.

100 партнёров-интеграторов системы

Продажи и внедрения системы с самого начала осуществляет сеть сертифицированных партнёров-интеграторов в разных регионах России и не только. В 2017 году партнёрская программа «ДоксВижн» признана одной из лучших среди разработчиков программного обеспечения (2-е место в рейтинге «Лучшая партнёрская программа в ИТ 2016» от ABD на TAdviser).

> Мы не просто разрабатываем продукт. Вокруг Docsvision сложилось целое сообщество наших коллег, заказчиков и партнёров – и это наш самый ценный ресурс. Мы делаем всё, чтобы каждый член этого сообщества имел всё необходимое для продуктивной работы и добивался успехов вместе с нами. Docsvision – это инструмент решения бизнес-задач.

100% российский софт

Импортозамещение сегодня – по-настоящему национальный проект, охвативший всю ИТ-отрасль, способный стать локомотивом её развития, а не просто средством заменить «чужое на своё».

Политика импортозамещения безусловно влияет на рынок СЭД/ECM, в первую очередь – на крупные госкорпорации. Если раньше в вопросах автоматизации документооборота и бизнес-процессов это была вотчина Documentum, то теперь в проектах участвуют и российские решения на платформах СПО, и полностью российские разработки на собственных российских платформах – таких как Docsvision.

Компания вовремя подготовилась к замещению западных ECM: возможности и достижения Docsvision в этом свете трудно переоценить.

- СЭД Docsvision включена в единый реестр отечественного программного обеспечения решением Экспертного совета при Минкомсвязи РФ, а компания «ДоксВижн» является членом АРПП «Отечественный софт».
- Docsvision – единственная отечественная платформа СЭД, прошедшая пилотный проект Минкомсвязи по переходу на отечественное офисное ПО на базе Минпрома РФ.
- Успешно проведено её нагрузочное тестирование на 100000 одновременных пользователей.
- В 2018 году выходит специальная редакция Docsvision ECM, масштабируемая до более 100000 одновременных пользователей и работающая на отечественной СУБД PostgreSQL.
- Сертификат ФСТЭК позволяет работать с системой компаниям с повышенными требованиями к безопасности.

В чём технологическое преимущество российской СЭД/ ECM платформы Docsvision

Low-code платформа
На базе платформы Docsvision можно решить целый ряд бизнес-задач компании и автоматизировать самые разные внутренние процессы – от делопроизводства и договорной работы до узких специализированных. В связи с цифровизацией экономики многие предприятия ищут единую платформу для хранения разнообразных видов документов и автоматизации соответствующих бизнес-процессов, выходящих за рамки «канцелярии» и базового делопроизводства.

Платформе Docsvision присуща гибкость, позволяющая менять готовые и создавать новые приложения без программирования: конструировать любые новые виды документов, их бизнес-логику, жизненный цикл и автоматизировать бизнес-процессы, интегрируясь в смежные информационные системы. В системе 10 визуальных конструкторов. Сегодня это становится решающим преимуществом.

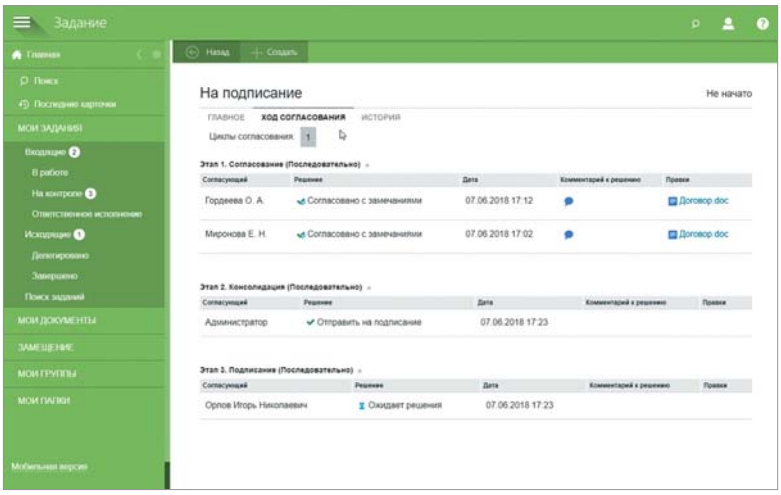
Комплексные решения от российских вендоров
Безусловно, для решения своих задач компания-заказчик может воспользоваться готовыми разработками на базе платформы – типовыми и специализированными решениями из каталога «ДоксВижн». Технологическое партнёрство с ведущими российскими вендорами – такими как ABBYY, «Новые облачные технологии», СКБ «Контур», FreshDoc, Postgres Professional, BEORG, НИИ «СОКБ», позволяет сразу предлагать комплексные решения по автоматизации документооборота и бизнес-процессов.

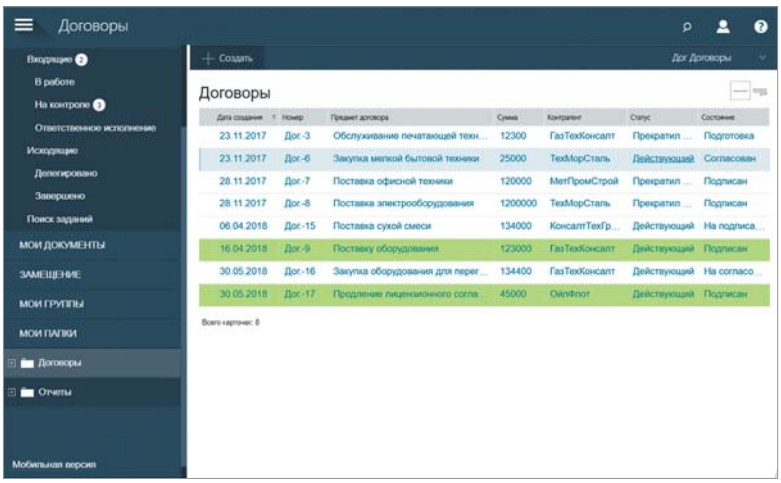
Интеграция и масштабируемость
Docsvision позволяет создавать централизованные и распределённые решения с возможностью одновременной работы до 100000 пользователей (и это не предел!). За счёт готовых интеграционных шлюзов СЭД Docsvision может быть интегрирована с другими корпоративными информационными системами без программирования.

Доступна интеграция с Microsoft SharePoint, «1С», Active Directory, любыми системами электронной почты, SAP, любыми операторами ЮЗДО. Любую внешнюю систему можно также интегрировать через XML- или веб-сервисы, используя открытый программный интерфейс (API).

Лёгкий и мобильный интерфейс
Пользователи могут работать в системе через веб-клиент, Windows-клиент, почтовый клиент. Вышло совершенно новое мобильное приложение «Пульс» для Android и iOS.

Анализ трендов рынка и требований компаний-заказчиков позволяет «ДоксВижн» делать современный мощный продукт для достойной замены любого зарубежного решения.





Docsvision

«ДоксВижн» – создатель и разработчик одноимённой платформы Docsvision, предназначенной для управления документооборотом и бизнес-процессами.

www.docsvision.com | info@docsvision.com

Индекс компании Gemalto – Identity and Access Management Index 2018

Проблемы в бизнесе

Сотрудники организаций заявили о необходимости сделать доступ к «облачным» хранилищам таким же, как для простых пользователей.

Две третьи руководителей ИТ-организаций сообщают о том, что в их компаниях начали упрощать доступ к облачным хранилищам в связи с ростом количества облачных приложений. Ежегодный опрос тысячи руководителей организаций по всему миру (Identity and Access Management Index) об управлении доступом, проведённый в 2018 году, показал, что способы аутентификации в большинстве компаний устарели, если сравнивать с такими сайтами, как Amazon или Facebook.

Сложность в процессе упрощения доступа состоит в том, чтобы не перестараться и сохранить безопасность доступа на должном уровне. ИТ- и бизнес-менеджеры стараются изо всех сил найти золотую середину между этими двумя крайностями. Одним из главных вопросов на повестке дня у них стоит проверка прочности защиты безопасности всех приложений, которые находятся в употреблении в их компаниях. Это поможет им выявить слабые места в защите приложений и понять, как именно нужно изменить методы доступа, чтобы убить сразу двух зайцев: сохранить достойный уровень безопасности и упростить доступ.

ЧАСТЬ 1

Чем руководствуются компании, выбирая методы управления доступом

Главным фактором всех времён, влияющим на решения по безопасности, был и остаётся риск взламывания приложений, содержащих сведения о потребителях.

Именно в связи с этим риском в 45% компаний стали выделять больше денег из бюджета на область безопасности. В 44% компаний теперь требуется ещё больше финансов на обучение работников программе безопасного доступа, в 42% компаний – на улучшение менеджмента доступом. А 38% – это 2/5 компаний – вынесли этот вопрос как самый важный на обсуждение в правлении компании. Если сравнивать с показателем 2016 года, то тогда он составил лишь 38%. А это значительная разница.

Таким образом, мы можем сделать вывод о том, как сильно повлиял рост количества взломов на принятия решений о безопасности в компаниях.

Какое влияние оказывают решения о потребительской аутентификации

По мнению 7/10 из тысячи опрошенных, ничего страшного не случится, если способы аутентификации для клиентов использовать также и внутри компании, поэтому неудивительно, что в 2 из 3 компаний уже ведётся работа по переходу от одного метода к другому. Тем не менее, всё ещё более чем в половине компаний аутентификация ни на миллиметр не приблизилась к аутентификации таких известных сайтов, как Facebook или Amazon.

Более чем в половине компаний аутентификация ни на миллиметр не приблизилась к аутентификации таких известных сайтов, как Facebook или Amazon.

Ещё одной проблемой является то, что персонал использует или может использовать личные данные во время работы. Однако несмотря на то, что руководители стремятся оправдать ожидания клиентов и сделать услуги удобными, безопасными и отвечающими всем современным трендам, риски, связанные с использованием личных данных, не установлены.

Риск использования личных данных в работе

В результате индекса стало очевидно, что социальные сети и платформы благотворительно влияют на торговлю. Известно, что и раньше недоброжелатели использовали данные из социальных сетей для взламывания корпоративных хранилищ данных, тем не менее до сих пор руководство не нашло идеального метода, обеспечивающего безопасный доступ к социальным сетям. Даже сейчас в двух из пяти компаний всё ещё вводят личные данные при создании учётной записи на работе.

Можем сравнить, что в 40% уже создали общий для всей компании аккаунт для использования социальных сетей в работе, в то время как в 30% компаний актуально использование личных данных в социальных сетях. Это ещё раз подтверждает тот факт, что ещё не найдён единый идеальный со всех сторон метод защиты данных.

92% опрошенных среди руководителей признают, что обеспокоены тем, что персонал использует личную информацию в работе.

Защита данных в соцсетях

В ходе опроса было выявлено, что чуть более чем в 50% организаций практикуют упрощённый метод защиты информации – обычный логин и пароль, в 2016 году это практиковалось в 65% компаний.

Ещё в 2016 году 42% компаний использовало двухфакторную аутентификацию на базе данных из соцсетей, сейчас же она используется в 40% компаний, а это значит, что её популярность уменьшается.

Каждая компания использует разные методы защиты данных, и в каждой компании есть один более популярный, чем другие.

ЧАСТЬ 2

Двухфакторная аутентификация

Как компании применяют двухфакторную аутентификацию

На данный момент в 40% опрошенных компаний применяется двухфакторная аутентификация, однако ожидается, что через два года уже 60% будут ею пользоваться.

По предварительным прогнозам, двухфакторная аутентификация будет набирать обороты, однако не отрицаются и возможные препятствия.

Защита «облачных» приложений двухфакторной аутентификацией

Двухфакторная аутентификация уже используется практически во всех компаниях (93%) – как минимум для одного приложения.

По данным индекса, для защиты «облачных» приложений двухфакторную аутентификацию используют почти 80% компаний (SaaS, PaaS, IaaS), для защиты локальной сети, интернет- и веб-порталов – 78%, для VPN и корпоративных приложений использует 77% компаний.

Подавляющее большинство компаний защищает около 3 приложений с помощью двухфакторной аутентификации, однако, согласно последнему исследованию Ponemon, всего в ИТ-компаниях в ходу около 27 «облачных» приложений.

Основные объекты атак хакеров

Как показывает практика, уязвимость защиты приложений и использование двухфакторной аутентификации взаимосвязаны – главным образом из-за того, считают руководители компаний, что именно такие приложения чаще всего интересуют хакеров. Веб-порталы считаются основным объектом атак хакеров для примерно половины опрошенных, «облачные» приложения, например, SaaS, PaaS, IaaS, – для 40% опрошенных, мобильные приложения – для 39%, доступ к корпоративным сетям – для 37%, а VPN считают уязвимым лишь 30%.

Также, по мнению 40%, очень часто взламывают незащищённые приложения – здесь чаще выделяют новинки от IoT. Итак, вопрос о защите доступа и общекорпоративной модели доступа, то есть которая подходила бы для любого отдела компании, остро стоит перед управляющими каждой компании, ведь неизвестно, какое приложение взломают следующим.

Чаще всего под угрозой взлома находятся незащищённые приложения и веб-порталы.

Двухфакторная аутентификация становится всё популярнее

По результатам опроса, управляющие практически единогласно ответили, что собираются расширить использование двухфакторной аутентификации в своих компаниях, при этом в большинстве компаний их популяр-

ность уже набирает обороты, поэтому они имеют возможность сделать значительный прыжок уже в течение года.

А если им в этом будет оказана помощь, темпы её распространения могут ещё больше вырасти.

О том, что они собираются расширять использование двухфакторной аутентификации, засвидетельствовали 96% глав ИТ-компаний.

Менеджмент двухфакторной аутентификации становится централизованным

Менеджмент двухфакторной аутентификации уже стал централизованным в более чем половине опрошенных компаний (58%), однако в более чем 30% этого ещё не произошло, но они к этому стремятся. Результат же прошлогоднего опроса был следующим: 46% уже управляли централизованно в 2016 году. Из чего мы видим, что это ещё далеко не предел.

Менеджмент двухфакторной аутентификации уже стал централизованным в 58% компаний, и этот процент продолжает расти.

Аудиты и соответствие нормам

Управляющие практически всех (тысячи) компаний сошлись во мнении, что в аудитах и поддержании норм в их компаниях большую роль играет двухфакторная аутентификация. Большая часть из них также считает, что для всех ресурсов в их организациях необходимо завести единый журнал аудита событий доступа, а о срочности этого события заявили около 30% опрошенных.

В основном, конечно же, возможность поощрять поддержание выполнения норм – это не главная причина перехода к двухфакторной аутентификации, однако лишней она точно не будет.

Управляющие практически тысячи компаний по всему миру сошлись во мнении, что в аудитах и поддержании норм (например, GDPR) в их компаниях большую роль играет двухфакторная аутентификация.

ЧАСТЬ 3

Менеджмент доступа к облачным приложениям (технология SSO в том числе)

Чаще всего хакеры взламывают облачные хранилища.

По мнению 40% опрошенных, чаще всего хакеров интересуют «облачные» хранилища.

Причиной этому 71% считает всё возрастающее количество таких приложений, 55% – недостаток соответствующих решений виртуальной безопасности. 40% считают, что всё-таки существуют определённые решения вопроса, касающегося защиты данных в «облачных» хранилищах, однако оно очень мало, что вполне поправимо.

Возрастающее количество «облачных» приложений считается главной причиной неспособности защитить их от хакеров.

Популяризация возможностей менеджмента доступа

Больше 40% компаний уже внедрили в свою систему безопасности «облачные» решения единого входа (SSO – Single Sign-on) для менеджмента доступа. Согласно результатам опроса, в 2016 году их доля равнялась 39%. Хотя разница и не большая, всё же распространение этого решения просматривается. О том, что «облачное» решение единого входа собираются внедрить в свою компанию, заявили 47% опрошенных. Более того, почти 60% руководителей подметили, что уже запущен процесс внедрения этого решения в их компаниях – в 2016 году их доля была на 47% меньше.

В 96% компаниях планируется внедрить двухфакторную аутентификацию для защиты корпоративных «облачных» хранилищ.

Основные факторы, повлиявшие на решение ввести менеджмент доступа и SSO

По результатам опроса стало известно, что боле 90% руководителей к введению менеджмента доступа подтолкнуло именно наличие проблем с защитой данных, а именно риск крупномасштабных взломов. Также 90% взволновали проблемы с видимостью и невыполнение требований в связи с событиями доступа к «облачному» приложению. Другие 88% взволновал иррациональный менеджмент идентификаций в «облачных» приложениях. Для 25% компаний самой главной причиной введения менеджмента доступа стала угроза крупномасштабного взлома и, что немаловажно, освещение в СМИ, что портит репутацию компании.

На решение ввести менеджмент доступа и SSO повлияло немалое количество факторов.

Технологии единого входа для «облачных» приложений (SSO)

Среди опрошенных 60% при выборе метода хранения данных отдают предпочтение «облачным» приложениям и лишь меньше 25% – локальным серверам. Факт того, что большую популярность имеют «облачные» хранилища – налицо.

Из них 40% уже имеют централизованный менеджмент SSO для всех приложений, а 50% выразили желание перейти к нему.

40% имеют централизованный менеджмент SSO для всех приложений, а 50% планируют перейти к нему.

Как в целом влияет на введение «облачных» хранилищ SSO

Положительный эффект менеджмента доступа на введение «облачных» хранилищ наблюдают практически все опрошенные, из которых 48% прямо-таки непоколебимы в этом вопросе.

Положительный эффект менеджмента доступа на введение «облачных» хранилищ наблюдают 91% опрошенных.

Следует также отметить, что, по мнению практически всех опрошенных, проблемы в компании может вызвать также и иррациональный менеджмент доступа к «облачным» хранилищам.

Например, по мнению 40% опрошенных, время сотрудников расходуется неразумно. Другие, кроме всего прочего, сообщают также об увеличении количества масштабных взломов, увеличении операционных накладных расходов и затрат на ИТ – именно из-за того, что отсутствует видимость «облака».

Нельзя не отметить масштабность влияния иррационального менеджмента доступа

ЧАСТЬ 4

Мобильность и внешние пользователи

Доступ к ресурсам и приложения компании для внешних пользователей

Для внешних пользователей при доступе к корпоративным ресурсам онлайн лишь в 43% компаний используется двухфакторная аутентификация, а в 46% компаний введение двухфакторной аутентификации пла-

нируется на ближайшее будущее, что свидетельствует о том, что эта ситуация ещё будет меняться.

Для внешних пользователей при доступе к корпоративным ресурсам онлайн лишь в 43% компаний используется двухфакторная аутентификация.

О политике доступа к ресурсам компаний

Руководители почти всех компаний единогласны во мнении, что в среднем 43% пользователей в их компаниях необходим удалённый доступ к приложениям компании. Практически в 90% компаний доступ к корпоративным данным с мобильных устройств частично ограничен, а полностью ограничен доступ к корпоративным данным с мобильных устройств лишь в 35% компаний, что не может не волновать.

В 36% компаниий уже перешли к политике использования двухфакторной аутентификации для защиты доступа к данным компании с мобильных приложений. В будущем же планируется, что доля этих компаний возрастёт до 57% за два года.

Практически в 90% компаний доступ к корпоративным данным с мобильных устройств частично ограничен. А в 36% компаний в целях защиты доступа к ресурсам компании для удалённых пользователей практикуется двухфакторная аутентификация.

Что мешает улучшить мобильность доступа

О препятствиях на пути к повышению мобильности пользователей говорят большинство опрошенных. Одни заявляют, что главной проблемой является ненадёжность системы безопасности, другие – что несоответствие данных, 40% – ограничительные нормы, 39% называют отсутствие общей видимости событий доступа, 27% – другое.

О наличии сложностей на пути к повышению мобильности пользователей говорят 95% опрошенных.

Способы аутентификации для сотрудников и клиентов

Один и тот же метод аутентификации клиентов и персонала используется в 40% компаний, в других 40% компаний для них популярны разные способы аутентификации.

Нередко в компаниях популярны разные способы аутентификации клиентов и сотрудников, что мы считаем нерациональным.

По мнению более чем 60% опрошенных, способы аутентификации клиентов и сотрудников компании всё больше приближаются друг к другу. 56% предположили, что уже через 3 года и клиенты и персонал будут использовать одни и те же данные для получения доступа к хранилищам. Всё это указывает на то, что скоро ситуация с аутентификациями в компаниях станет совершенно другой.

Актуальные способы аутентификации

До сих пор в качестве аутентификации среди 69% служащих большую популярность имеют системы логинов и паролей. Она, можно сказать, затмевает все остальные методы. Тем не менее даже через два года не предвидится большой рост этой доли пользователей, максимум до 71%.

В то время как с биометрической аутентификацией положение вещей абсолютно противоположное. Предполагается, что процент пользователей вырастет с 25% до 44% всего за 2 года. Всё это свидетельствует о приближении к эре более современных способов аутентификации.

Также, по данным опроса, около 30% сотрудников широко используют программные и аппаратные ключи. Ставки делаются на то, что за ближайшие 4 года их доля вырастет значительно, половина служащих будет пользоваться программными токенами, а 46% – аппаратными ключами.

Кроме того, ещё большие обороты (от 30% до 40%) наберёт популярность аутентификации по внешнему каналу, аутентификации без использования маркеров и учётных данных социальных сетей.

По результатам опросов в 2016 и 2017 годах, показатели популярности вышеперечисленных способов аутентификации практически не отличаются.

Демографическая составляющая индекса

В 2017 году (сентябрь-ноябрь) для опроса 1050 управляющих различных ИТ-компаний со всего мира были разделены на группы в зависимости от их страны, вида предоставляемых услуг и количества сотрудников и опрошены.

Как влияют на политику управляющих атаки хакеров и рост популярности «облачных» приложений

С появлением многообразия различных «облачных» и локальных хранилищ у компаний появилось не только много плюсов, но это также вызвало и ряд трудностей, связанных с не меньшим разнообразием способов менеджмента их безопасности. Если менеджмент иррационален, появляются такие проблемы, как взломы, отсутствие видимости событий доступа, сложности удалённого нормативного регулирования и сложности роста организаций за счёт «облачных» приложений.

90% опрошенных заявили, что из-за взломов им пришлось поработать над своей политикой безопасности. В связи с этим большую ответственность стал нести главный директор по информационной безопасности, а в 58% компаний появились новые решения менеджмента доступа к аккаунтам.

Исследование Вансона Борна

Вансон Борн является независимым специалистом в исследовании конъюнктуры рынка в технологическом секторе. У нас чистая репутация, заслуженная точными анализами кропотливо собранных данных, ведь мы всегда прислушиваемся к мнениям старших руководителей по техническим и бизнесвопросам, какой бы то ни был сектор бизнеса или основной рынок.

www.vansonbourne.com

Gemalto SafeNet

Компания Gemalto предоставляет большой спектр решений для защиты данных в компаниях, являясь ведущей компанией в сфере безопасности цифровых данных, транзакций, платежей и идентификаций и многого другого.

Именно благодаря таким нашим проектам, как SafeNet Identity и Data Protection, компании самых разнообразных направлений предоставляемых услуг имеют возможность использовать самые современные способы шифрования данных, криптографические способы менеджмента и решения строгой аутентификации, менеджмент идентификационными данными. Всё это помогает любым, даже крупным финансовым или государственным институтам, сохранить то, что важно, чтобы воспользоваться в тот момент, когда это важно. Также, наши решения позволяют в этом оцифрованном мире соблюдать регламент конфиденциальности и охранить в безопасности секретные корпоративные данные, данные о клиентах и транзакциях. И будьте уверенны, что клиент к вам ещё вернётся.

www.gemalto.com

Назад в будущее

Российский рынок ИКТ

До этого полугодия некоторые аналитики, руководители крупных дистрибьюторов и других российских ИТ-компаний не раз высказывали мнение, что российский ИТ-рынок в 2016 году стабилизировался. Некоторые эксперты даже утверждают, что в конце года был заметен рост рынка. Однако ни одна из исследовательских компаний не представила свои оценки по объёму всего российского ИТ-рынка на конец 2016 года. Напомним, что «Руссофт» этим исследованием рынка не занимается. Аналитики ассоциации делают вывод об эффективности ИТ-рынка только на основании данных, взятых из множества других источников (отчёты исследовательских компаний, опубликованные рейтинги, официальные данные крупнейших российских ИТ-компаний).

«Руссофт» на основе наших исследований может оценить точность измерения рынка ПО, так как у нас есть информация о продажах российских разработчиков ПО на внутреннем рынке.

Ещё 5-10 лет назад можно было бы проанализировать объём всего российского ИТ-рынка по 3-4 исследовательским компаниям, включая IDC и Gartner. А ещё немного раньше эта информация была публично представлена только IDC. В конце 2016 года они также исчезли. Судя по всему, интерес зарубежных аналитических компаний к российскому ИТ-рынку упал, а в свою очередь российские исследователи, которые смогли бы охватить весь рынок, так и не проявили себя.

Министерства связи и массовых коммуникаций, экономического развития и торговли то и дело представляют свои данные, однако всё указывает на то, что государственные служащие ограничиваются пересчётом показателей IDC (или Gartner) в рубли с поправкой на инфляцию (или без неё), а также самостоятельно определяют, какие решения и услуги относятся к ИТ-рынку.

Несмотря на то, что IDC впервые не опубликовала основной индикатор российского ИТ-рынка, его объём можно рассчитать на основе информации о сегментах рынка, которая могла быть собрана в различных изданиях. Получается, что в долларах падение рынка ИТ по итогам 2016 года составило порядка 3-4%. По сравнению с падением на 39% в 2015 году это сокращение можно по праву назвать стабилизацией, что и сделали аналитики IDC.

В то же время в 1-м полугодии 2016 года они прогнозировали падение рынка ИТ по итогам года на 13%. «Руссофт» прогнозировал рост ИТ-рынка на 2-3% или такое же снижение, но в рублях. Аналогичный показатель в долларах США прогнозировался в зависимости от курса рубля по отношению к доллару. Фактически, национальная валюта снизилась в стоимостном выражении примерно на 10%, а спад рынка ИТ (если руководствоваться IDC) оказался гораздо меньше.

Справедливо предположить, что в 2016 году наблюдался даже небольшой рост рынка ИТ в долларовом эквиваленте. Есть веские основания полагать, что это было так, будто совокупный оборот 100 крупнейших компаний в долларах в рейтинге TAdviser100 сократился на 1,5% (и вырос на 4,7% в рейтинге CNews), но небольшие софтверные компании, которые не могли попасть в эти рейтинги, увеличили продажи на внутреннем рынке в рублях на 36% (по расчёту «Руссофт» на основе ежегодных опросов).

Судя по итогам года, отечественных и зарубежных софтверных компаний этот рынок не только не сократился, но даже вырос на 11-12% (в долларах США).

ИТ-рынок с точки зрения различных участников рынка

Давайте с самого начала опираться на данные IDC, которые говорят о том, что предполагаемый объём российского ИТ-рынка должен быть не менее 17 миллиардов долларов. При этом все его крупные сегменты (оборудование, программное обеспечение, ИТ-услуги) сократились на 3-5%, поэтому широкая структура российского ИТ-рынка не стала принципиально иной.

Если разбить его на более мелкие фрагменты, то изменения будут значительными, так как одни фрагменты показали значительный рост, а другие – значительное сокращение.

В пересчёте на рубли рынок ИТ вырос на 5,1%, что примерно соответствует официальному уровню инфляции в 5,4%. Поэтому в рублёвом выражении и в сопоставимых ценах объём рынка остаётся прежним.

Существует также оценка рынка ИТ, которую осуществило Министерство экономического развития и торговли, но только в виде прогноза, опубликованного осенью 2016 года. По предположению госслужащих, рынок ИТ по итогам года должен был сократиться в сопоставимых ценах на 1,7%, то есть до 747,4 млрд рублей (11,2 млрд долларов США). Но, судя по всему, они не учли последний (достаточно успешный для продажи ИТ-компаний) квартал, а также такой растущий и крупный сегмент ИТ-рынка, как СП.

Если рассматривать объём ИТ-рынка в долларовом выражении, а также данные по многим сегментам и другим показателям, то можно провести дополнительный анализ. Необходимость в этом вызвана тем, что «Руссофт», в отличие от зарубежных аналитиков, смотрит на внутренний рынок не только с позиций вендоров, которых интересует только валютная выручка. С другой стороны, «Руссофт» учитывает интерес других важных игроков рынка, в том числе пользователей ИТ (как физических, так и корпоративных клиентов ИТ-компаний), а также отечественных компаний, в том числе и особых союзников «Руссофт» – софтверных компаний.

Для российских пользователей важно получить от ИТ-рынка определённую полезную функциональность. Даже если мы допустим, что они получат эту функциональность бесплатно (то есть при нулевом размере соответствующего рынка), они выжмут из него максимум, хотя зарубежные аналитики заявят о крахе ИТ-рынка. Что касается ИТ-продуктов или услуг, невозможно получать выгоду бесплатно (даже бесплатное ПО, как правило, требует платной поддержки),

Таблица 1. ИТ-рынок России в 2013-2017 годах

		2013	2014	2015	2016	2017 (прогнозы)
С точки зрения зарубежн. компаний	В долл. (рост/падение в год)	$33 млрд (-1 %)	$28 млрд (-16 %)	$17,8 млрд (-39 %)	≈$17 млрд (-3-4 %)	$18,5-20,5 млрд (+10-20 %)
С точки зрения отечеств. компаний	В рублях (рост/падение в год)	₽1,05 млрд (+3,9 %)	₽1,063 млрд (+1,2 %)	₽1,08 млрд (+1,6 %)	₽1,137 млрд (+5,3 %)	₽1,19-1,25 млрд (+5-10 %)
	Изменение в рублях с поправкой на офиц. Инфляцию	-2,4 %	-9,1 %	-9 %	≈0 %	+0-5 %
С т. зр. росс. пользователей	Бивалютный индекс «Руссофт»	-	-10,6 %	-25 %	≈0 %	+5-10 %

Источник: рассчитано по данным IDC.

но снижение цен в области ИТ не редкость. Это приводит к уменьшению размера рынка и расширению возможностей для получения большей функциональности за те же деньги.

Сложно оценить функциональность и преимущества в контексте всего ИТ-рынка, однако можно сделать предположения о её качественном изменении. Тем более что существуют и количественные оценки для некоторых сегментов рынка (количество устройств, совокупная мощность и т.д.).

Изменения состояния ИТ-рынка для пользователей можно в какой-то мере оценить по бивалютному индексу «Руссофт» – с учётом изменения цен в долларах и рублях. Таким образом, хотя и с низкой точностью, можно определить тенденции и значимость изменений.

Поскольку было бы некорректно определять влияние ИТ на экономику и общество, исходя из оценки объёма рынка в определённой валюте (зависит как от цен в долларах, так и в рублях), «Руссофт» разработал метод определения индекса, который позволяет вести учёт процесса в разных валютах.

Суть заключается в следующем. Рынок делится на импортные и отечественные решения, и рост в соответствующей валюте определяется для каждого сегмента отдельно. Затем учитывается удельный вес каждого сегмента. Доля российских компаний за год увеличилась незначительно, поэтому мы можем игнорировать её изменение в наших расчётах.

Для российских компаний важен размер ИТ-рынка, но в основном они измеряют выручку в рублях. Поэтому для них важнее ёмкость рынка в рублёвом выражении.

Вслед за этим методологическим введением можно напомнить, как изменился объём российского ИТ-рынка в предыдущие годы. Высокие темпы роста в несколько десятков процентов были характерны для периода с 2000 по 2008 год включительно. Это время закончилось мировым финансовым кризисом, негативно повлиявшим на российскую экономику. В результате после длительного периода роста в 2009 году российский ИТ-рынок сократился на 16% в долларовом выражении. Уже в конце 2010 года после неплохого роста рынок вернулся к прежнему уровню – докризисный объём рынка в долларовом выражении был быстро превышен.

Однако после кризиса топ-менеджеры ИТ-компаний заявили, что российский рынок для них изменился раз и навсегда, поскольку корпоративные заказчики коренным образом скорректировали свои программы проникновения ИТ и закупочную политику (*таблица 1*).

Очередной рост ИТ-рынка остановился в 2013 году с символическим снижением на 1% (по данным IDC), однако речь всё же не шла об экономическом кризисе. Ситуацию в следующие два года аналитики международных исследовательских компаний охарактеризовали как крах ИТ-рынка. По их мнению, он завершился в 2016 году, а в 2017 году они ожидали значительного роста. Однако эта история российского ИТ-рынка представлена с позиций иностранных корпораций. Во время мирового кризиса 2009 года, ещё 7 лет назад, это подтверждалось тем, что такой предвзятый взгляд не позволял адекватно оценить ситуацию в целом. В 2010 году никто не мог сказать, что шок предыдущего года тяжело отразился на российской экономике в целом и на IT-индустрии в частности. Инвестиции в информационные технологии стали более вразумительными и продуманными, в то же время многие софтверные компании, которые раньше быстро росли на внутреннем рынке, стали смотреть на страны, не входящие в СНГ, где продажи обеспечивали большую стабильность. Подводя итоги 2013 года, выяснилось, что стагнация, которая была выявлена во время символического сокращения объёма ИТ-рынка в долларах США, с точки зрения пользователей была мифической. Ни о каком упадке не может быть и речи. Очевидно, что в России кипела деятельность в области информационного обеспечения. Некоторые сегменты выросли на 10% и более, другие сократились на 10%. Анализ этих изменений показал, что

более дешёвые технологии (нередко лучшие для пользователей) вытесняли те, которые требовали больших затрат. Прежде всего это было продемонстрировано достаточно масштабным переходом к «облачным» технологиям. Кроме того, необходимо учитывать значительное удешевление компьютерной техники и наметившуюся тенденцию перехода к свободным ПО. Таким образом, предполагалось, что пользователи в 2013 году получили больше полезных функций, чем годом ранее.

Между тем проявился ещё один фактор – грядущая перегрузка ряда условных сегментов ИТ-рынка. Например, подключённые к интернету компьютеры были почти в каждом доме, а ERP и EDMS – почти в каждом предприятии, где их раньше не было.

«Руссофт» выделил следующие факторы, которые, помимо макроэкономических проблем, определили в 2013-2016 гг. сокращение российского ИТ-рынка в долларовом выражении:

1) повышение эффективности инвестиций в ИТ (наибольшее влияние в наиболее критичные для экономики годы);

2) появление альтернативных технологий, включая общее программное обеспечение;

3) перегрузка некоторых традиционных сегментов;

4) снижение долларовых цен (для компьютерной техники);

5) отсутствие сенсационных товаров (есть все основания полагать, что доступность масштабного внедрения широкого спектра новых технологий позволит в ближайшее время забыть об этом факторе).

Если непредвзято взглянуть на текущую историю ИТ-рынка с точки зрения пользователей (с точки зрения влияния на отечественную экономику), а также на историю российских ИТ-компаний, то можно назвать годом спада в полном смысле этого слова только 2015 год. Только в этом году пользователи получили от ИТ-индустрии явно меньшую функциональность, чем в предыдущем (тем не менее они получили достаточно много, поскольку даже ограниченные расходы на ИТ позволили не только поддерживать уже работающие системы и оборудование, но и обеспечить их развитие). С учётом изменения рынка одновременно в рублях и в долларах США по бивалютному индексу с точки зрения пользователей рынок сократился на 25%. Этот показатель не учитывает замену одних технологий другими и переход на свободные программы, но даже с учётом этих процессов падение всё равно было значительным – в лучшем случае примерно на 10%.

В отношении 2016 года такой твёрдый вывод о сокращении ИТ-рынка с точки зрения пользователей сделать уже нельзя. Произошло либо незначительное сокращение, либо небольшое увеличение (в зависимости от сегмента рынка).

Для российских ИТ-компаний, оценивающих свои неудачи и успехи в рублях, за последние 16 лет не произошло ни одного сокращения рынка в рублёвом выражении. Даже в 2014-2015 годах рынок вырос на символическую величину. В действительности, если учитывать официальную инфляцию, то в конечном итоге произошло значительное сокращение за этот период (на 9,1% и 9% соответственно). В 2013 году в сопоставимых ценах в рублях рынок ИТ также несколько снизился, но это падение было более чем компенсировано тем, что российские компании захватили определённую долю рынка ИТ у иностранных поставщиков.

Вопрос о необходимости поэтапного отказа от импорта в Россию в 2013 году обсуждался не так активно, как в следующие два года, но всё же он шёл с постепенным ростом доли российских компаний в некоторых сегментах отечественного ИТ-рынка.

Следовательно, с точки зрения российских компаний можно говорить о существовании кризиса на внутреннем рынке только в отношении 2014 и 2015 годов. Особенно сложным был 2015 год, когда оборот ряда российских компаний даже в рублёвом выражении сократился на десятки процентов. В то же время такое падение в какой-то степени свидетельствовало о восстановлении рынка (т. е. о вполне благоприятной ситуации). Например, компании, которые предлагали «облачные» решения, наслаждались ростом эти 2 года. И действительно, продажи разработчиков внутри России несколько выросли – даже с учётом официального уровня инфляции (в долларах они так или иначе потеряли позиции).

Возможно, беспорядки на внутреннем рынке даже укрепили российскую индустрию программного обеспечения, а не ослабили её. Более того, российские компании получили больше импульсов для работы на мировом рынке.

Подводя итоги 2016 года, только зарубежные вендоры могут говорить о кризисе на российском ИТ-рынке. Даже для них напряжение оказалось безобидными. Некоторым поставщикам с таким сокращением в России даже удалось увеличить продажи в долларах. Количество ИТ-пользователей и российских ИТ-компаний в 2016 году заметно увеличилось.

В этом контексте, несмотря на общее сокращение рынка ИТ в долларовом выражении (по версии IDC), большинство его сегментов пережили значительный рост. Падение сосредоточено только в тех сегментах, которые сокращаются и на всём мировом рынке. Такая усадка говорит о насыщении этих сегментов или внедрении новых технологий, но не о кризисных явлениях на рынке.

Данные IDC несомненны, однако справедливо предположить, что методология этой глобальной исследовательской компании разрабатывается в первую очередь с учётом информации тех же глобальных корпораций, имеющих значительную долю рынка по всему миру. Можно предположить, что конкретные местные сегменты ИТ-индустрии в разных странах могут быть недооценены.

В любом случае, оценки продаж российских компаний по разработке ПО на внутреннем рынке говорит о том, что на рынке продуктов разработчиков программного обеспечения (в том числе продаж лицензионного ПО, продаж разработок, услуг установки и ремонта, а также предоставление ПО как услуги) в России гораздо выше, чем по показателю в отчётах IDC (для получения дополнительной информации, пожалуйста, обратитесь к соответствующему подразделу на российском рынке ПО). Собственные данные по рынку ПО позволяют «Руссофт» предположить, что объём российского ИТ-рынка должен составить не 17 млрд долларов США, а не менее 20 млрд долларов США.

Кроме того, по итогам 2016 года можно сделать вывод не только

о стабилизации российского ИТ-рынка, но и о его очевидном расширении с точки зрения отечественных ИТ-компаний и IT-пользователей. Его можно выстроить в ряд на 5-10%. Такой рост для отечественных компаний с практически неизменным размером рынка в рублёвом выражении (с поправкой на инфляцию) означает снижение доли иностранных корпораций и предложенную нами недооценку отдельных сегментов российского ИТ-рынка в части IDC. Для пользователей цены в 2016 году как выросли, так и снизились, а рост обеспечил переход на «облачные» технологии и свободные программы.

Принципиально важно, что выводы «Руссофт» и IDC не расходятся. Они отличаются лишь тем, что в одном случае на ИТ-рынок смотрели российские компании и российские ИТ-пользователи, а в другом – иностранные вендоры. Тем более что именно IDC остаётся источником наиболее полного представления о российской ИТ-среде. Расчёты и выводы «Руссофт» определённо и во многом основаны на данных этой компании.

К сожалению, в России нет такого релевантного внутреннего реферального источника о рынке ИТ. Для государственной статистики (Росстата) сектора ИТ и рынка ИТ вообще не существует. Деятельность в области статистики ещё не переориентирована на текущую рыночную экономику с быстро развивающимися высокотехнологичными компаниями. Это можно увидеть в представленной статистической информации, которая появляется с большой временной задержкой (иногда в течение 1,5-2 лет, когда ситуация в экономике и разных отраслях может быть совершенно разной) и в той же форме, которая была подготовлена много лет назад для контролируемой государством экономики. Об этом свидетельствует также отсутствие в статистических отчётах многих важных показателей, характеризующих развитие высокотехнологичного сектора экономики.

Минкомсвязи России в лице своего представителя ещё в июле 2014 года выступило с заявлением: «На данный момент в России нет официальных единых статистических показателей для ИТ-отрасли, поэтому с точки зрения официальной статистики такой отрасли не существует».

Регулятор предложил разработать единый порядок оценки эффективности Российской ИТ-отрасли, по итогам которого подготовлен проект приказа Министерства. Однако прошло три года, и о результатах этого предложения ничего не известно.

Штаб-квартира «Руссофт» в Санкт-Петербурге предприняла попытку получить от Росстата информацию об общих доходах софтверных компаний Санкт-Петербурга с разъяснением источника данных, но даже запрос, сделанный на платной основе, был проигнорирован.

Некоторые сведения позволяют сделать вывод о том, что происходит на российском ИТ-рынке

По данным TAdviser, всего расходы всех государственных органов (федеральных и региональных) составляют 12-13% от всего объёма российского ИТ-рынка.

ИТ-бюджет российских федеральных органов власти составляет 0,6% от общей суммы федерального бюджета РФ (16,1 трлн рублей). В США этот показатель составляет 2,2%.

По данным OCS Distribution, одной из крупнейших российских дистрибьюторских компаний, российский ИТ-рынок стабилизировался и по итогам 2016 года может вырасти на 2-3% в долларовом выражении. Этот прогноз был дан в самом конце года, поэтому он должен быть достаточно точным.

Импортозамещение, по данным OCS Distribution, стало ньюсмейкером уже в 2016 году, но будет гораздо более значительным в ближайшие годы. Бизнес многих российских вендоров с продукцией в портфеле дистрибьюторской компании растёт быстрее 10% в год. Это касается не только поставщиков, но и отечественных производителей оборудования (*таблица 2*).

Таблица 2. Итоги 2016 года ряда российских и зарубежных компаний

Название	Профиль	Рост/падение товарооборота в рублевом рублёвом выражении
Docsvision	Разработчик Docsvision системы для документооборота и управления бизнес-процессами на предприятиях и в организациях	+30/40 %
Группа ALP	ИТ-аутсорсинг	Оборот отдела ИТ-аутсорсинга увеличился в 1,5 раза. В 1,8 и 2,3 раза увеличились направления деятельности розничная торговля и работа с открытыми исходными
Интелтелеком	Разработчик систем в области автоматизация обработки вызовов в России и странах СНГ	рост > 30 %

Продолжение на следующей странице.

Название	Профиль	Рост/падение товарооборота в рублевом рублёвом выражении
Vocord	Разработчик и производитель профессиональных инструментов для видеонаблюдения и телекоммуникационных решений	+7/9 %
Система	Международная компания, разработчик профессиональных инструментов электронного обучения, онлайн-презентаций и организации дистанционного обучения	+100 %
Oblakoteka	«Облачная» платформа на IaaS	+70 %
Syssoft	Мультисервисный провайдер и SI, поставщик «облачных» решений, программного и аппаратного обеспечения в России и странах СНГ	Рост > 90 %
EDCOM	Поставка интерактивного оборудования, 3D-принтеров, роботизированных модулей и компьютерной техники для образовательных учреждений, учебных центров и коммерческих компаний	Рост > 100 %
Код Безопасности	Разработчик программного и аппаратного обеспечения, средства защиты информации	+29,5 %
Информационная безопасность	Российский холдинг, специализирующийся в области информационной безопасности автоматизированных систем управления	+31 %
Netlab	Дистрибьютор компьютерной техники и комплектующих	+43 %
OCS Distribution	Дистрибуция компьютерной сетевой телекоммуникационной периферии комплектующих бытовой техники	+23 %
Распределения Marvel	дистрибьютор полного спектра ИТ	Рост > 10 %
Продажи иностранных компаний в России		
QNAP (Тайвань)	Поставщик и разработчик беспроводных сетевых устройств	+20 %
TP-Link (Китай)	Поставщик беспроводной сети	+32 %
САП СНГ (Германия)	Техника	+11 %
SAS (США)	Разработчик технологического программного обеспечения	Рост > 40 %
IBM (США)	Производитель и поставщик аппаратного и программного обеспечения	–20 %
Apple (Россия) – филиал в России	Производитель персональных и планшетных компьютеров, аудиоплееров, телефонов, программного обеспечения	+70 %

Начало на предыдущей странице.

Структура российского ИТ-рынка

Доля ИТ-услуг в 2014-2015 гг. заметно увеличилась с 20% до 25% (в 2016 г. она существенно не изменилась). Это свидетельствует о том, что рынок становится всё более зрелым, хотя это изменение в первую очередь было вызвано значительным ростом стоимости импортного оборудования, что привело к сокращению продаж. Если оценивать ситуацию с точки зрения российских пользователей и российских вендоров, то всё указывает на то, что общая доля ИТ-услуг и программного обеспечения в объёме российского ИТ-рынка составляет более 38% и может достигать 45% (*таблица 3*).

Информация о сегменте российского ИТ-рынка

Если по итогам 2015 года подавляющее большинство сегментов российского ИТ-рынка сокращалось, то в 2016 году картина совсем другая – преобладает рост, причём в некоторых сегментах рост у нас очень высокий – на десятки процентов (*таблица 4*).

Что касается внешнего рынка хранения данных: если в долларовом выражении это всё ещё на достаточно низком уровне 2015 года, то общая ёмкость системы увеличилась почти на 40%. Это означает, что иностранные компании, занимающиеся поставками, имели лишь номинальный рост продаж в России, но пользователи получили гораздо большую функциональность за те же доллары, чем год назад.

Примечательно существенное различие в информации о рынке ПК между IDC и ITResearch. Если в количестве проданных компьютеров разница не слишком велика (вероятно, это объясняется разными методологиями), то в изменении этой суммы в течение года разница огромна: IDC зарегистрировал падение на 7,9%, в то время как ITResearch – рост на 1%.

Спад на рынке серверов IDC трактует как развитие сегмента «облачных» сервисов и технологий виртуализации сервисов. Рынок «облачных» услуг растёт на десятки процентов в год (*таблица 5*).

Российский рынок программного обеспечения

Российский рынок программного обеспечения достиг максимального размера в 2013 году и составил 5 млрд долларов США (по версии IDC).

Таблица 3. Структура российского ИТ-рынка на конец 2016 года

	Абсолютное значение	Изменение	Доля
ИТ-оборудование	$10,6 млрд	–34%	62%
ИТ-услуги	$4,27 млрд	–5,3%	25%
Программное обеспечение	$2,208 млрд	–4%	13%
Итого:	$17,1 млрд	–4%	100%

Источник: рассчитано по данным IDC.

Таблица 4. Отдельные сегменты российского ИТ-рынка

Индикатор	2016	Падение (-)/рост (+) на конец 2016 года	Источник
Аппаратура			
Российский рынок внешние системы хранения данных (общий объём)	$382,77 млн (663002 ТБ)	+0,5% (+35,7%)	IDC
Российский рынок ПК	4,47 млн шт.	–7,9%	IDC
Российский рынок ПК (настольный компьютер и ноутбук)	5,084 млн шт.	+1%	ITResearch
Русский рынок планшетов	4,71 млн шт.	–22,9% (–27,8% в $)	IDC
Российский рынок серверов	102033 шт. ($531,3 млн)	–4,5% (–20,1%)	IDC
Российский рынок принтеров	2,28 млн шт. ($489.78 млн)	+0,4% (+11%)	IDC
Русские «умные» часы	–	+11% в шт. (+44% в ₽)	M. Video
Планшетный компьютер	4,9 млн шт.	–24% (–14%)	ITResearch
Принтеры и настольные МФУ	2,2 млн шт.	–11,9%	ITResearch
Мониторы	2,33 млн шт. ($369 млн)	+10,6% (+5,4%)	ITResearch
ИБП	1,08 млн шт. ($292,6 млн)	+4,5% (+9,2%)	ITResearch

Продолжение на следующей странице.

Индикатор	2016	Падение (-)/рост (+) на конец 2016 года	Источник
Программное обеспечение			
Объём российского рынка компьютерной техники игр	₽97,5 млрд	+13,7%	Компания J'son & партнеры
Российский рынок ОРЭД	$632,72 млн (₽42,2 млрд)	–1,1% (+8,8% в рублях)	IDC
Услуги			
Количество клиентов службы виртуального обмена	149,9 тыс.	+26%	iKS-Consulting
Российский рынок ИТ-услуг	$4,27 млрд	–5.3% (+3.6% в рублях)	IDC
Российский рынок IaaS	₽8,07 млрд	+37%	SAP, Forrester (Россия), 2017
Российский рынок SaaS	₽13,79 млрд	+48%	SAP, Forrester (Россия), 2017
Фьючерсный рынок			
Число российских компаний, работающих в AR/VR	183 (105 – в Москве, 25 – в Санкт-Петербурге)	+205%	AVRA
Расходы на продукты и услуги, относящиеся к интернету вещей (Internet of Things IoT)	₽85 млрд ($1,2 млрд)	+42% (+29%)	AC&M Consulting
Доход российских операторов от IoT	₽7,6 млрд	+25%	AC&M Consulting

Начало на предыдущей странице.

Таблица 5. Объём российского рынка «облачных» технологий в 2014-2017 годах (рост в год)

	2014	2015	2016	2017 (прогноз)
SaaS	₽6,95 млрд (+46%)	₽9,3 млрд (+34%)	₽13,79 млрд (+48%)	₽13,79 млрд (+23%)
IaaS	₽4,75 млрд (+57%)	₽5,87 млрд (+24%)	₽8,07 млрд (+37%)	₽10,1 млрд (+25%)

Источник: SAP, Forrester Russia, 2017.

В последующие два года она снизилась более чем в два раза – до 2,3 миллиарда долларов. В 2016 году свободное падение прекратилось. Судя по данным СМИ, упоминаемым IDC, рынок программного обеспечения сократился ещё на 4%. Таким образом, она снизилась до 2,2 млрд долларов США, однако, по оценкам «Руссофт» (на долю которого приходится реализация как продуктов, так и услуг российских компаний-разработчиков), продажи российских компаний-разработчиков на внутреннем рынке составляют 4,4 млрд долларов США. С учётом результатов ежегодного опроса «Руссофт», вероятно, что на практике этот показатель выше (примерно на 1-2 миллиарда долларов).

Разработка заказного программного обеспечения, которое IDC сравнивает с рынком ИТ-услуг, составляет 1,3 млрд долларов США. Здесь у нас нет прямого противоречия, поскольку объём услуг по разработке программного обеспечения составляет 30% всего российского рынка ИТ-услуг (4,3 млрд долларов США). Тем не менее от продаж тиражированных решений остаётся 3 млрд долларов США.

Отчасти утверждение о том, что результаты продаж российских софтверных компаний оказываются больше, чем весь рынок программного обеспечения (по данным IDC), можно объяснить двойным подсчётом, так как при разработке решения на платформе определённого вендора оплата этому вендору учитывается дважды – в доходе конечного разработчика решения и в доходе разработчика платформы. Однако этот двойной показатель едва ли превышает 0,5 млрд долларов США.

Кроме того, 3 млрд долларов США совокупных продаж программного обеспечения российскими софтверными компаниями на внутреннем рынке скрывает выручка от деятельности на других рынках. Например, разработчики стандартных тиражируемых решений продают не только программные продукты, но и аппаратно-программные комплексы, и оборудование на базе собственного программного обеспечения. Монетизация мобильных приложений может осуществляться через рекламу. Эти доходы софтверных компаний на других рынках также вряд ли превысят 0,5 млрд долларов США.

В любом случае объём продаж российских софтверных компаний на отечественном рынке не меньше, чем объём всего рынка. В то же время в России продаётся и зарубежное программное обеспечение, на которое приходится как минимум 1,5-2 миллиарда долларов. Поэтому весь рынок программного обеспечения должен составлять не менее 4-5 млрд долларов, а при заказной разработке – не менее 6-7 млрд долларов.

При этом методологии, цели и задачи исследования отдельных рынков могут существенно отличаться. Действительно, существует большое количество методов измерения рынка программного обеспечения. Следовательно, существуют серьёзные расхождения в результатах исследований. Должны ли мы включать специальное программное обеспечение в понятие «рынок программного обеспечения» или нет? Считать ли SaaS ИТ-услугами или программным обеспечением? Должны ли мы учитывать доходы софтверных компаний от внедрения и поддержки или нет? Если компания разрабатывает специальное программное обеспечение для конкретного клиента, но на собственной реплицированной платформе, это услуга или стандартное решение? Если софтверная компания продаёт серийно выпускаемые программно-аппаратные комплексы на базе своего стандартного программного обеспечения, представляет ли она продажу оборудования или программного обеспечения? Таких вопросов очень много. В большинстве случаев методологические трудности по-прежнему связаны с вопросом о том, входит ли тот или иной сегмент в рынок ИТ-услуг или в рынок программного обеспечения.

Поэтому и 2,2 млрд долларов, и 6-7 млрд долларов могут быть одновременно вполне корректными оценками российского рынка программного обеспечения. Возможно, IDC учитывает только лицензионные сборы, а чаще 30-40% выручки от продажи программных продуктов компании попадает в эту часть, а остальные доходы разработчики получают за поддержку и другие услуги.

Помимо отличной от IDC оценки абсолютного размера российского рынка программного обеспечения, «Руссофт» по-разному оценивает его изменение. Различные данные показывают, что сокращение продаж программного обеспечения в 2016 году маловероятно в любых единицах измерения. Российские разработчики программного обеспечения увеличили продажи на внутреннем рынке в среднем на 16%. При этом рост был достигнут в долларах, а в рублях рост составил 28%. Зарубежные софтверные компании, раскрывшие показатели продаж, заявляют, что выручка в России и СНГ в долларах США либо осталась прежней, либо увеличилась. Например, рост SAP составил 1%, A SAS – более 25%.

Таблица 6. Основные характеристики российского рынка программного обеспечения в 2015-2016 годах

	2015	2016	Комментарий
Объём рынка (изменение за год)	$2,3 млрд (–43.1%)	$2,2 млрд (–4%)	Версия IDC
	$5,56,4 млрд (–30-32%)	$67 млрд (+11-12%)	Версия «Руссофт»
Изменения в рублях с учётом официального уровня инфляции	–19%	+16-17%	Версия «Руссофт»

На самом деле многие софтверные компании, в том числе зарубежные, пересмотрели рублёвые цены на свои программные продукты. В частности, компания Microsoft в начале 2017 года опережала курс рубля, девальвированного по отношению к доллару в течение 2016 года. Эта ценовая ревизия показывает, что компания Microsoft также сократила продажи в России.

Возможно, сокращение имело место в продаже лицензий, но это никак не связано с экономической ситуацией в России, так как программное обеспечение оставляет товарную категорию в категорию услуг. Компании-разработчики в массовом масштабе сокращают долю выручки от продажи лицензий и увеличивают долю от продажи услуг, аналогичных SaaS, которые IDC, скорее всего, включает с ИТ-услугами.

На российском рынке заказного программного обеспечения преобладают местные разработчики. Их совокупный доход от продаж на внутреннем рынке составил 1,3 млрд долларов США, увеличившись в 2016 году на 13%. Можно утверждать, что весь соответствующий сегмент вырос на те же 13%.

Может случиться так, что после получения более полной информации о рынке программного обеспечения его объём может быть скорректирован вперёд – до 8-9 млрд долларов. Предположим, что в России работают 3 тыс. компаний-разработчиков программного обеспечения (по всей видимости, более) – это указывает на то, что российские компании продают на внутреннем рынке программного обеспечения на сумму 6,3 млрд долларов США (без двойного счёта). К этому показателю следует добавить как минимум 1,5-2 млрд долларов, которые иностранные компании получили от продаж в России.

Рост российского рынка ИТ-услуг в долларовом выражении в 2016 составил 11-12%, а в рублях – 22-23%.

Для пользователей программного обеспечения ситуация улучшилась, хотя рост цен на программное обеспечение значительно превысил официальный уровень инфляции (5,4%). Рост расходов на программы в значительной степени компенсировал рост тарифов, но пользователи получили дополнительные функциональные возможности за счёт перехода на свободные программы и SaaS (*таблица 6*).

RUS®SOFT

«Некоммерческое Партнерство РУССОФТ» *– крупнейшее объединение компаний-разработчиков программного обеспечения России.*

www.russoft.ru

ИТ-конференция по информационной безопасности

Концепция мероприятия – объединение вендоров, продуктов и решений с максимальным эффектом для клиента.

CISummIT

ПРИГЛАСИТЕЛЬНЫЙ БИЛЕТ

Для бесплатного участия на мероприятии «CISummIT» сделайте всего два шага:

1. Перейдите по QR-коду и заполните форму регистрации
2. Оторвите пригласительный билет (справа) и приходите на конференцию

25 октября 2018

«Москва-Сити»

Заполните регистрационную форму для участия на мероприятии

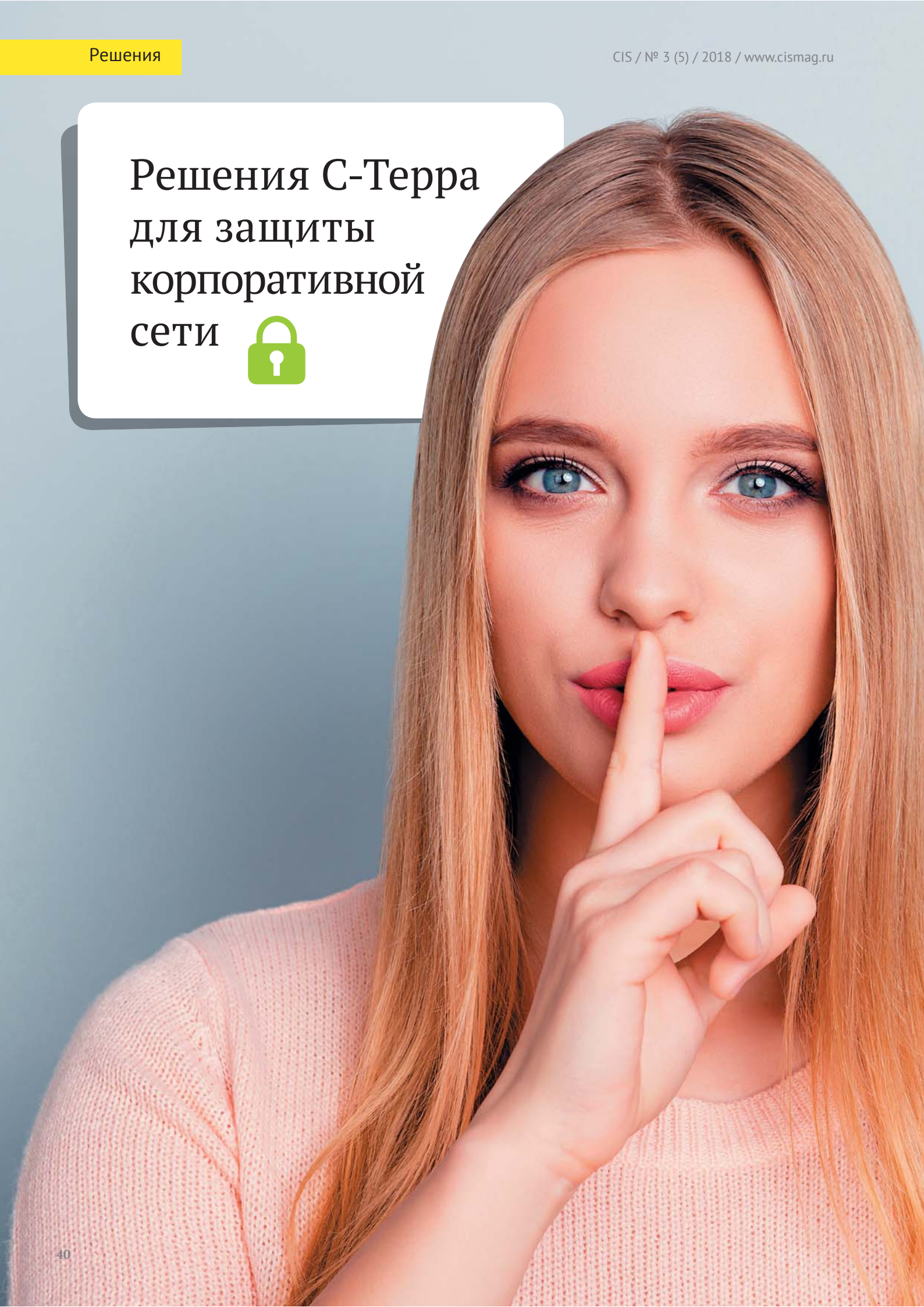
www.cismag.news

CIS Современные Информационные Системы

www.cismag.news


CIS

Решения С-Терра для защиты корпоративной сети



Любая организация заботится о сохранении своей информации, т. к. её разглашение может нанести ущерб как самой организации, так и другим лицам. Такую информацию называют конфиденциальной.

С этимологической точки зрения слово «конфиденциальный» происходит от латинского confidentia – доверие. В современном русском языке это слово означает «доверительный, не подлежащий огласке, секретный».

С развитием информационных технологий задача обеспечения информационной безопасности и, в частности, конфиденциальности приобретает всё большую значимость. Она крайне важна для любой организации, а для некоторых областей регламентируется на государственном уровне. Если в информационной системе обрабатывается информация, подлежащая обязательной защите в соответствии с российским законодательством (например, персональные данные – ПДн), то необходимо использовать сертифицированные средства защиты, прошедшие процедуру оценки регуляторами. В связи с этим российский рынок средств информационной безопасности является достаточно специфичным. Проведение сертификации под силу не каждой компании – необходимо быть лицензиатом ФСБ России и ФСТЭК России.

Компания «С-Терра СиЭсПи» основана в 2003 году и является ведущим российским разработчиком и производителем средств сетевой информационной безопасности, специализирующимся на разработке и производстве средств криптографической защиты информации (СКЗИ) на основе российских криптоалгоритмов ГОСТ и стандартов IKE/IPsec (RFC2401-2412). Архитектура IPsec проверена многократным технический анализом и тестированием специалистов многих стран и внедряется по всему миру, в том числе и в России. Все продукты сертифицированы ФСБ России как средства криптографической защиты информации (СКЗИ) по классам КС1, КС2, КС3, а также во ФСТЭК России. Продуктовая линейка компании активно расширяется и позволяет решить множество задач, при этом соблюдая требования законодательства.

Продукты С-Терра используются в государственных и банковских организациях, в федеральных и региональных органах законодательной и исполнительной власти, в силовых структурах, крупных промышленных корпорациях, небольших коммерческих организациях.

Использование оборудования С-Терра позволяет решить целый ряд задач:

- защита филиальной сети различного масштаба и топологии;
- защищённый доступ удалённых сотрудников;
- защита высокопроизводительных каналов связи между ЦОД;
- защита доступа к виртуальной инфраструктуре;
- подключение к СМЭВ;

и прочих.

Защита территориально распределённых сегментов

Современный бизнес не ведётся в пределах офисных стен: компоненты инфраструктуры большинства компаний географически распределены. При этом им необходимо единое информационное пространство для создания которого используются, в том числе, недоверенные каналы связи. Для обеспечения конфиденциальности и целостности информации, передаваемой по таким каналам, необходимы VPN-продукты.

Компания «С-Терра СиЭсПи» предлагает широкую линейку шлюзов безопасности «С-Терра Шлюз», которые обеспечивают защиту трафика при его передаче, а также межсетевое экранирование. В центральной точке шлюзы могут работать в отказоустойчивой конфигурации для обеспечения беспрерывного сервиса.

Линейка шлюзов безопасности масштабируется от миниатюрных устройств, размером чуть больше спичечного коробка, до полноценных серверов, предназначенных для защиты десятков гигабит трафика. Это позволяет найти оптимальное по производительности решение для любой задачи, будь то защита взаимодействия офисов, IP-телефонии, видеоконференцсвязи и т.д.

Защита удалённого доступа

Множество организаций требуют от сотрудников постоянно находиться на связи и быть готовыми отреагировать в сжатые сроки на любые виды запросов. Компании привлекают сотрудников из других городов, регионов, даже стран. Удалённо работающие сотрудники – это тоже сегмент корпоративной сети, и ему нужна защита.

Для решения этой задачи на удалённое рабочее место устанавливается программное обеспечение – «С-Терра Клиент» (для всех современных ОС Windows) или «С-Терра Клиент-М» (для ОС Android). Продукты обеспечивают защиту трафика как внутри сети, так при передаче по внешним каналам связи. Поддерживается режим изоляции

от внешних сетей с помощью туннелирования всего трафика в корпоративную сеть с выходом в интернет через отдельный прокси-сервер. Также могут быть использованы дополнительные факторы аутентификации, например, токены и аутентификация на RADIUS-сервере.

Защита высокопроизводительных каналов между ЦОД

ЦОД стали чрезвычайно привлекательной мишенью для злоумышленников. Особенно перспективной точкой взлома выглядят магистральные волоконно-оптические каналы связи, соединяющие различные ЦОД, ведь через них передаётся колоссальное количество данных. При этом устройства съёма данных с волоконно-оптических каналов без разрыва волокна стоят всего лишь несколько сотен долларов. С их помощью злоумышленники могут в режиме реального времени получать доступ к передаваемым данным, а также собирать информацию для будущих атак.

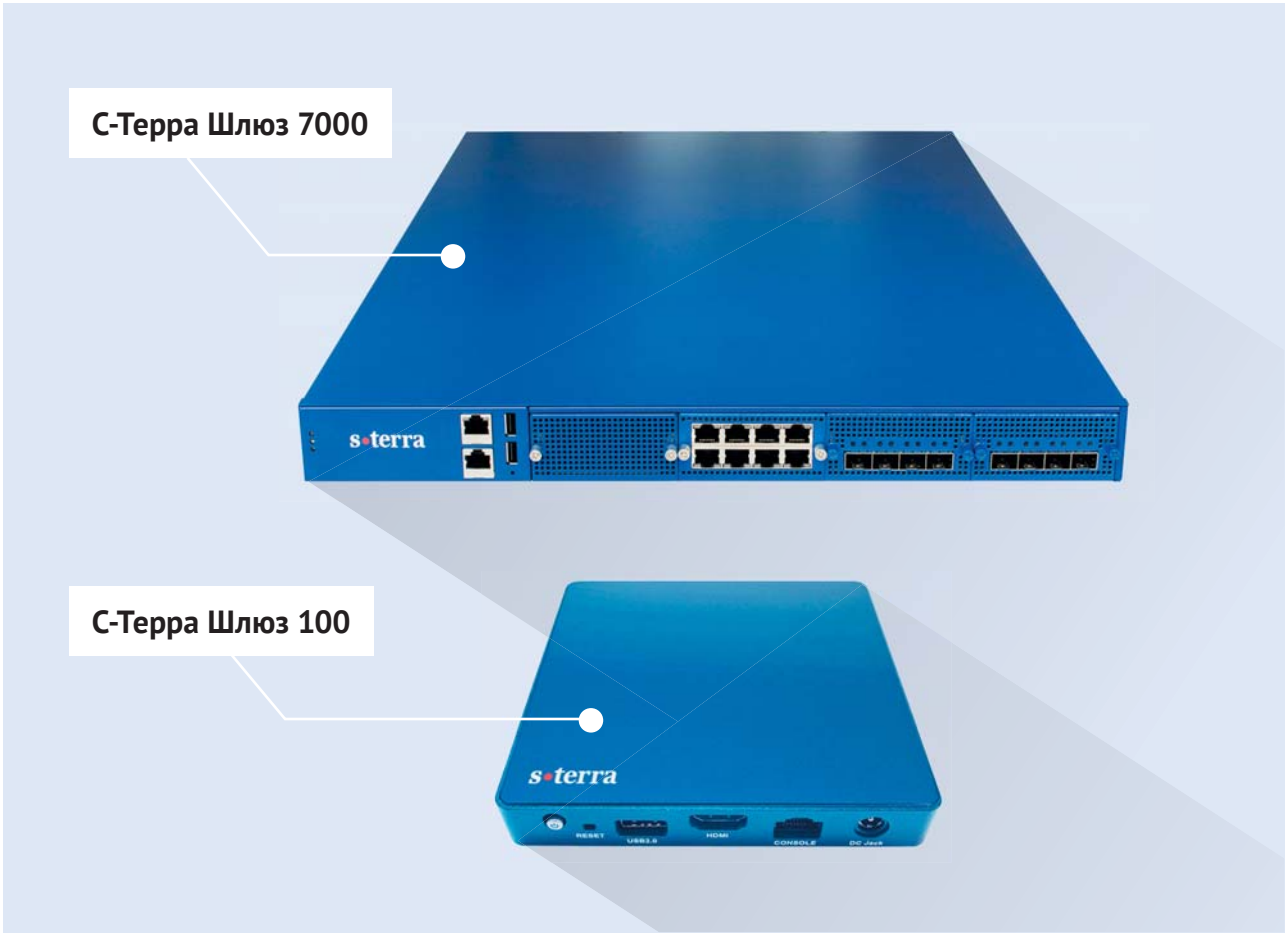
Становится очевидно, что каналы, соединяющие ЦОД между собой, необходимо защищать как от пассивного вмешательства (т.е. прослушивания данных), так и от активных действий злоумышленников (т.е. попыток изменить передаваемую информацию или не допустить её передачи). Когда ЦОД географически удалены друг от друга, физическая защита становится очень дорогой, а зачастую совсем невозможной. В такой ситуации приходится использовать недоверенные каналы связи и необходимо применять криптографическую защиту передаваемых данных.

Компания «С-Терра» предлагает комплексное решение на базе сертифицированных VPN-устройств «С-Терра Шлюз 10G» и коммутаторов, обеспечивающих балансировку трафика. Решение позволяет организовать высокопроизводительный защищённый канал между центрами обработки данных на скоростях от 10 Гбит/с и выше.

Минимальный комплект состоит из четырёх шлюзов безопасности и набора документации. Для его применения требуется наличие двух коммутаторов, соответствующих определённым требованиям: поддержка протокола LACP или PAgP, наличие необходимого количества интерфейсов 10 Гбит/с. Шлюзы используются для построения защищённого туннеля связи на канальном уровне. Такой туннель позволяет обеспечить конфиденциальность и целостность передаваемых данных даже в том случае, если промежуточное оборудование на канале было взломано злоумышленником. Коммутаторы выступают в роли балансировщиков трафика, обеспечивая масштабируемость и отказоустойчивость решения. Для балансировки трафика коммутаторы используют агрегированный канал (LACP или PAgP). Главные преимущества решения – отказоустойчивость и масштабируемость.

Защита доступа к виртуальной инфраструктуре

Использование дополнительных аппаратных VPN-шлюзов для защиты доступа к виртуальной среде не всегда целесообразно. Непосредственное встраивание в виртуальную среду позволяет в полной мере использовать основные преимущества технологии виртуализации: экономичность, масштабируемость, отказоустойчивость, а также позволяет



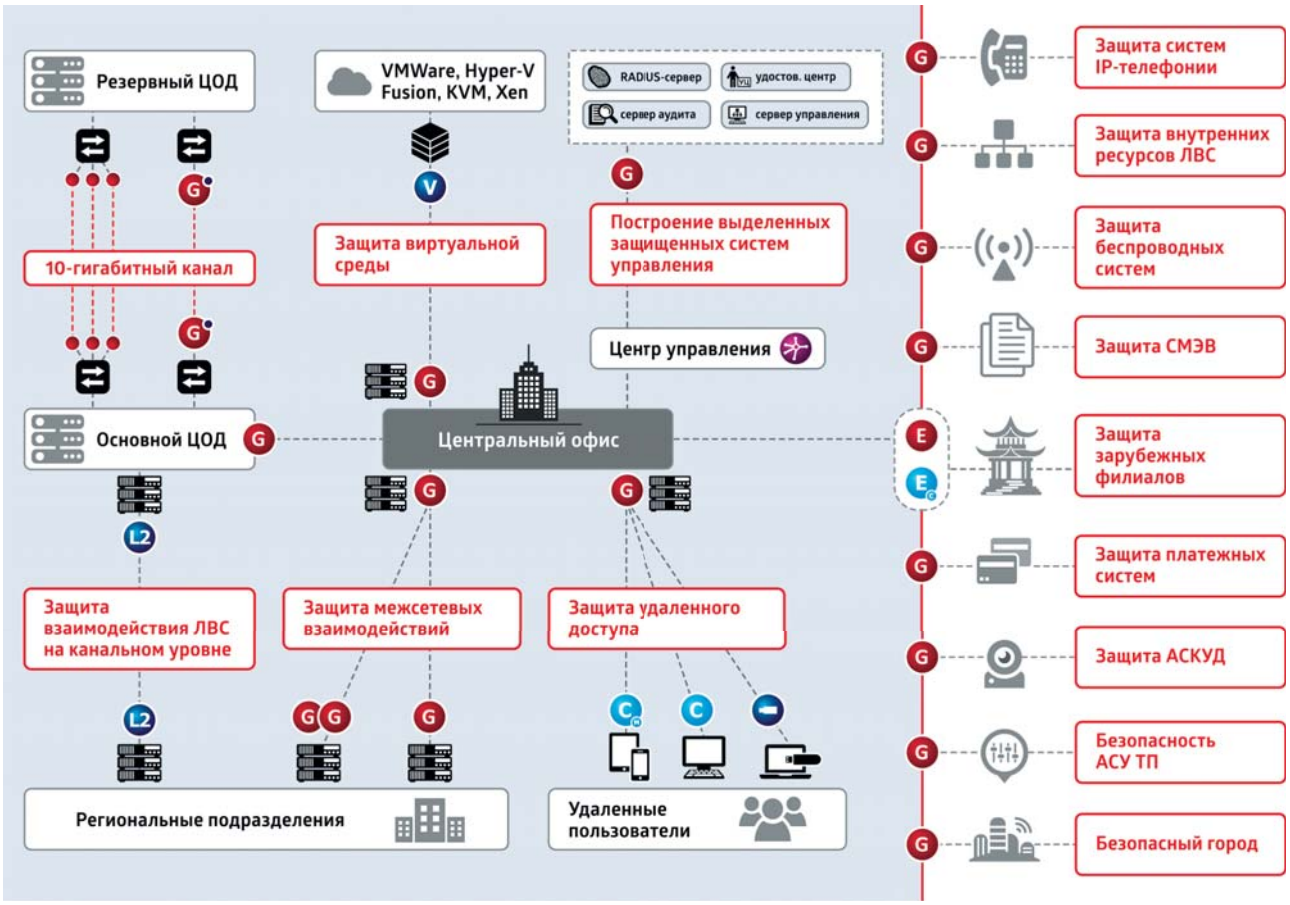


Схема решений.

избежать неудобств, возникающих при эксплуатации программно-аппаратных комплексов. Средства защиты, выполненные в виде виртуальных программных комплексов, имеют аналогичную функциональность, не уступающую традиционным программно-аппаратным решениям, при этом повышая удобство пользования сетевыми сервисами и упрощая администрирование средств защиты информации.

В линейке «С-Терра» этот подход реализован в продукте «С-Терра Виртуальный Шлюз». Это виртуальная машина для гипервизоров VMware ESXi, Citrix XenServer, MS Hyper-V, KVM, HW Fusion с функциональностью полноценного аппаратного криптошлюза «С-Терра». Виртуальный шлюз сертифицирован ФСБ России по классу КС1, а также во ФСТЭК России. Производительность зависит от частоты процессора аппаратной платформы и лицензии, которая ограничивает количество ядер, используемых для шифрования. К заказу доступны лицензии на 1, 4 и 12 ядер. Гибкий лицензионный механизм позволяет подобрать оптимальный вариант шлюза под любую задачу, а при необходимости – повысить производительность. На данный момент это уникальный для российского рынка продукт.

Подключение к СМЭВ

Приказом Минкомсвязи России от 23.06.2015 № 210 установлены Технические требования к взаимодействию информационных систем в СМЭВ, которые, в частности, предусматривают использование для обеспечения сетевой защиты данных набора протоколов IPsec, а также защиту всех каналов связи, выходящих за пределы контролируемых зон участников взаимодействия, с помощью сертифицированных средств криптографической защиты информации (СКЗИ) класса не ниже КС3.

Для организации подключения пользователей в федеральном центре обработки данных СМЭВ – на площадке ПАО «Ростелеком» – установлены криптошлюзы компании «С-Терра СиЭсПи».

При подключении к системе заказчик самостоятельно приобретает «С-Терра Шлюз» необходимой производительности для своей площадки, далее передаёт его для управления и поддержки операторам системы – сотрудникам ПАО «Ростелеком».

Резюме

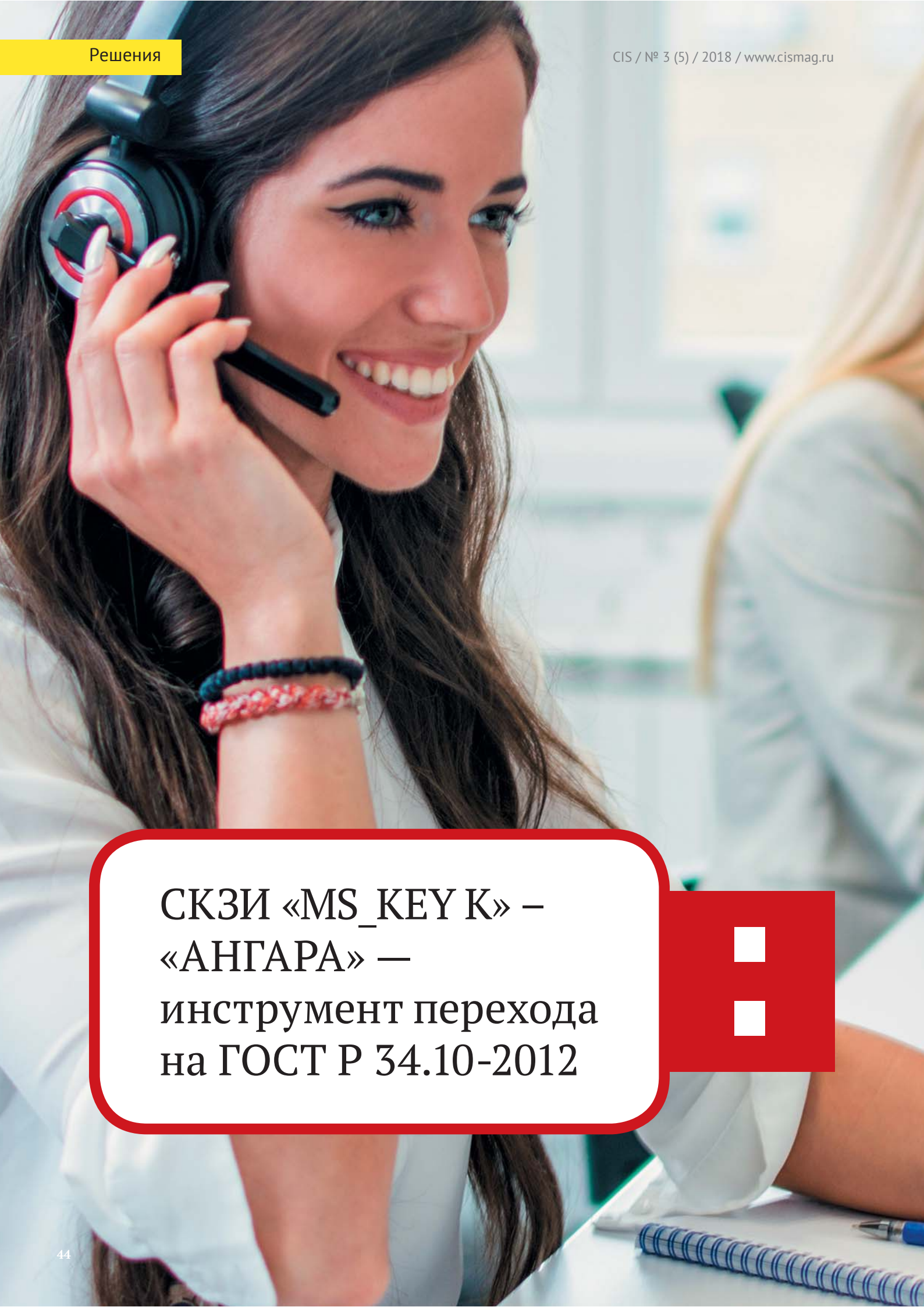
«С-Терра СиЭсПи» является одним из лидеров рынка отечественных VPN-продуктов. Компания предлагает решения, соответствующие всем современным техническим требованиям в области информационной безопасности и позволяющие обеспечить выполнение требований регуляторов в сфере информационно безопасности. Именно такой подход обеспечивает надёжную защиту любой информационной системы.

Веселов Александр,
руководитель отдела технического консалтинга ООО «С-Терра СиЭсПи»

s·terra®
ВАШ ОРИЕНТИР В МИРЕ БЕЗОПАСНОСТИ

***«С-Терра СиЭсПи»** – российский разработчик и производитель средств сетевой информационной безопасности.*

www.s-terra.ru



СКЗИ «MS_KEY K» – «АНГАРА» — инструмент перехода на ГОСТ Р 34.10-2012

В 90-х годах XX века с появлением большого количества программ по автоматизации делопроизводства началось активное внедрение электронного документооборота, способствующего повышению эффективности использования рабочего времени и уменьшению затрат времени на обработку документов на бумажном носителе.

На сегодняшний день создаваемые с помощью средств компьютерной обработки информации электронные документы стали неотъемлемой частью нашей жизни. Важным атрибутом электронного документа является электронная подпись (ЭП). Она используется в системах электронного документооборота, сбора налоговой и статистической отчётности, при аутентификации на государственных и коммерческих веб-порталах, в единой государственной автоматизированной информационной системе (ЕГАИС), в системах дистанционного банковского обслуживания (ДБО). ЭП позволяет определить, кем и когда был подписан документ, обнаружить факт внесения в него изменений после подписания, обеспечивает юридическую значимость такого документа. При этом электронная подпись, как и сам электронный документ, требует защиты.

Обеспечение защиты ЭП – важный элемент системы информационной безопасности. Несмотря на то, что подделка ЭП, особенно квалифицированной электронной подписи, является трудноразрешимой задачей для злоумышленников, с развитием вычислительной техники повышается вероятность её компрометации. В связи с этим повышаются и требования, предъявляемые к формированию и проверке ЭП. Приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 года № 215-ст стандарт ГОСТ Р 34.10-2001 введён запрет на использование схемы ГОСТ Р 34.10-2001 после 31 декабря 2018 года. Взамен ГОСТ Р 34.10-2001 был создан новый отечественный стандарт – ГОСТ Р 34.10-2012, в соответствии с которым для средств ЭП должна быть предусмотрена реализация функций хотя бы по одному из определяемых стандартом вариантов требований к параметрам (при этом использование варианта, соответствующего длине секретного ключа порядка 256 бит, является предпочтительным, поскольку обеспечивает достаточный уровень криптографической стойкости и лучшие эксплуатационные характеристики).

Ещё одной угрозой, связанной с ЭП, является хищение закрытого ключа, которым подписываются документы. Для обеспечения защиты от подобного вида атак компания «МультиСофт Системз», являющаяся крупнейшим отечественным разработчиком программно-аппаратных средств криптографической защиты информации на базе интеллектуальных карт, предлагает использовать технологию неизвлекаемых ключей ЭП. При её использовании генерация ключевой пары происходит внутри аппаратного криптопровайдера и закрытый ключ не покидает устройство (ключевой носитель).

Примером такого устройства является средство криптографической защиты информации нового поколения СКЗИ «MS_KEY K» – «АНГАРА», которое отвечает всем требованиям ФСБ России, предъявляемым к СКЗИ по классам защиты КС1 и КС2, а также требованиям к средствам ЭП по классам КС1 и КС2. На изделие выданы сертификаты соответствия ФСБ № СФ/124-3072 (форм-фактор USB-токена), СФ/124-3296 (форм-фактор смарт-карты). В СКЗИ «MS_KEY K» – «АНГАРА» реализована аппаратная поддержка как новых криптоалгоритмов: ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 (в режимах 256 и 512 бит), так и ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001, что делает для пользователей СКЗИ «MS_KEY K» Исп.5.x.x переход на новое поколение наиболее прозрачным и комфортным.

Помимо ассиметричного шифрования, на устройстве реализованы блочные крипто-алгоритмы: ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015 и ГОСТ 28147-89, что является выгодной отличительной особенностью и делает его привлекательным для работы в системах межмашинного взаимодействия (M2M) и других, где необходимо аппаратное шифрование.

Вместе с тем необходимо отметить, что для повышения уровня безопасности при осуществлении операций в системах ДБО могут использоваться устройства класса TrustScreen, являющиеся доверенной средой между компьютером и носителем ключевой информации. Отображение на экране устройства реквизитов платежа обеспечивает защиту от подмены документов.

Различные форм-факторы и интерфейсы делают СКЗИ «MS_KEY K» – «АНГАРА» простым для встраивания и удобным в использовании средством обеспечения информационной защиты.

MultiSoft

Группа компаний МультиСофт *объединяет в себе два успешных проекта: ООО «МультиСофт Системз» и ООО «НТЦ Альфа-Проект».*

www.multisoft.ru

multisoft@multisoft.ru

CIS / № 3 (5) / 2018 / www.cismag.ru

Комплексная безопасность корпоративных сетей на платформе UserGate

В последние годы многие крупные организации вынуждены заменять различные зарубежные решения, особенно из тех, что обеспечивают функции информационной безопасности. Есть несколько причин, вызывающих необходимость такой замены. В ряде случаев зарубежные вендоры не производят продление лицензий на используемые в России решения. В других случаях, даже когда есть техническая возможность продлять подписки на используемые решения, возникают вопросы относительно доверия к продуктам, которые не получают сертификацию ФСТЭК России и потенциально могут подвергать опасности критически важную инфраструктуру. В данной статье пойдёт речь о решениях, обеспечивающих комплексную защиту корпоративных сетей на уровне шлюза, то есть на узлах сети. Наиболее популярными сейчас в России производителями из этой категории являются американские компании Palo Alto Networks, Fortinet, McAffee и израильская компания Check Point.

Несмотря на объективную необходимость перехода на отечественные решения, компании не могут начинать использовать системы, не могущие обеспечивать тот же уровень функциональности, безопасности и производительности, к которому они привыкли. На рынке присутствует множество «отечественных» решений, по сути являющихся просто слегка модифицированными разработками с открытым кодом.

В силу вышеописанных причин выбор российских компаний всё чаще и чаще ложится на UserGate. Этот продукт уже стал обеспечивать безопасность предприятий самого разного размера с числом пользователей до 20 тысяч. Во многих проектах UserGate успешно замещает ранее использовавшиеся зарубежные аналоги. С 2016 года данное решение успешно используется как в органах власти, так и на предприятиях финансовой, энергетической, производственной, агропромышленной сфер, в образовании и здравоохранении, в розничных сетях и на других вертикальных рынках.

UserGate является комплексным решением по обеспечению безопасности компьютерных сетей любого размера. В его основе лежит операционная система UG OS, обеспечивающая всестороннюю и высокопроизводительную защиту, а также специально адаптированная и оптимизированная аппаратная часть.

UserGate обеспечивает межсетевое экранирование для предприятий любого размера, поддерживая при этом высокую скорость обработки трафика, многоуровневую безопасность, применение гранулярных политик к пользователям и прозрачное использование интернет-канала. Аппаратные и виртуальные межсетевые экраны UserGate предоставляют многочисленные возможности по управлению функциями безопасности, обеспечивают прозрачность относительно использования трафика и интернета со стороны пользователей, устройств и приложений.

Уникальная архитектура UserGate и операционная система UG OS позволяют обрабатывать и анализировать сетевой трафик на самых высоконагруженных каналах связи и добиваться эффективного масштабирования. Интеграция множества функций безопасности на единой платформе и применение модульного подхода даёт возможность удобной настройки решения под специфические запросы любого заказчика.

UserGate содержит все функции решений класса UTM (Unified Threat Management), обеспечивая безопасность от всевозможных интернет-угроз и управление интернет-доступом для организаций малого и среднего размера. Работа функций безопасности решения основана на постоянном взаимодействии с центром безопасности, что позволяет поддерживать минимальное время реакции на известные и неизвестные угрозы. Разработчики UserGate, обслуживая большое число именно российских пользователей, обладают специфическим опытом по работе с интернет-ресурсами и угрозами, особенно актуальными для русскоязычного сегмента интернета. UserGate осуществляет защиту от атак, управление трафиком, аутентификацию интернет-пользователей, а также обеспечивает безопасность посещения сотрудниками интернет-ресурсов, ограждает их от загрузки опасного и вредоносного содержимого.

Система обнаружения и предотвращения вторжений (IPS – Intrusion Prevention System) позволяет реагировать на атаки злоумышленников, использующих известные уязвимости, а также распознавать вредоносную активность внутри сети.

Технологии, используемые в UserGate, соответствуют современной концепции SOAR (Security Automation, Orchestration and Response), позволяют анализировать поведение различных процессов, выявлять риски и автоматически обеспечивать на основе этого анализа адекватную реакцию, обеспечивая защиту от угрозы или просто от аномального поведения на самой ранней стадии. Администратор может задавать сценарии и ответные действия на события, что сокращает время между обнаружением угрозы и ответом на неё, а также приоритизировать события, обеспечивая своевременную реакцию на критические атаки.

Обеспечение сетевой безопасности становится всё более сложной проблемой из-за постоянного появления новых угроз и увеличения объёма данных, связанных с инцидентами безопасности. Для решения этой проблемы необходимо использование продвинутых средств, позволяющих анализировать разнообразные данные, такие как записи в журналах безопасности.

UserGate Log Analyzer предоставляет дополнительные возможности по анализу данных об инцидентах безопасности, их мониторингу, сбору статистики и созданию отчётов. Решение может быть развёрнуто отдельно от шлюза безопасности и в состоянии агрегировать данные из нескольких источников. Разделение функций обработки трафика и анализа данных позволяет обеспечить лучшую надёжность и масштабируемость.

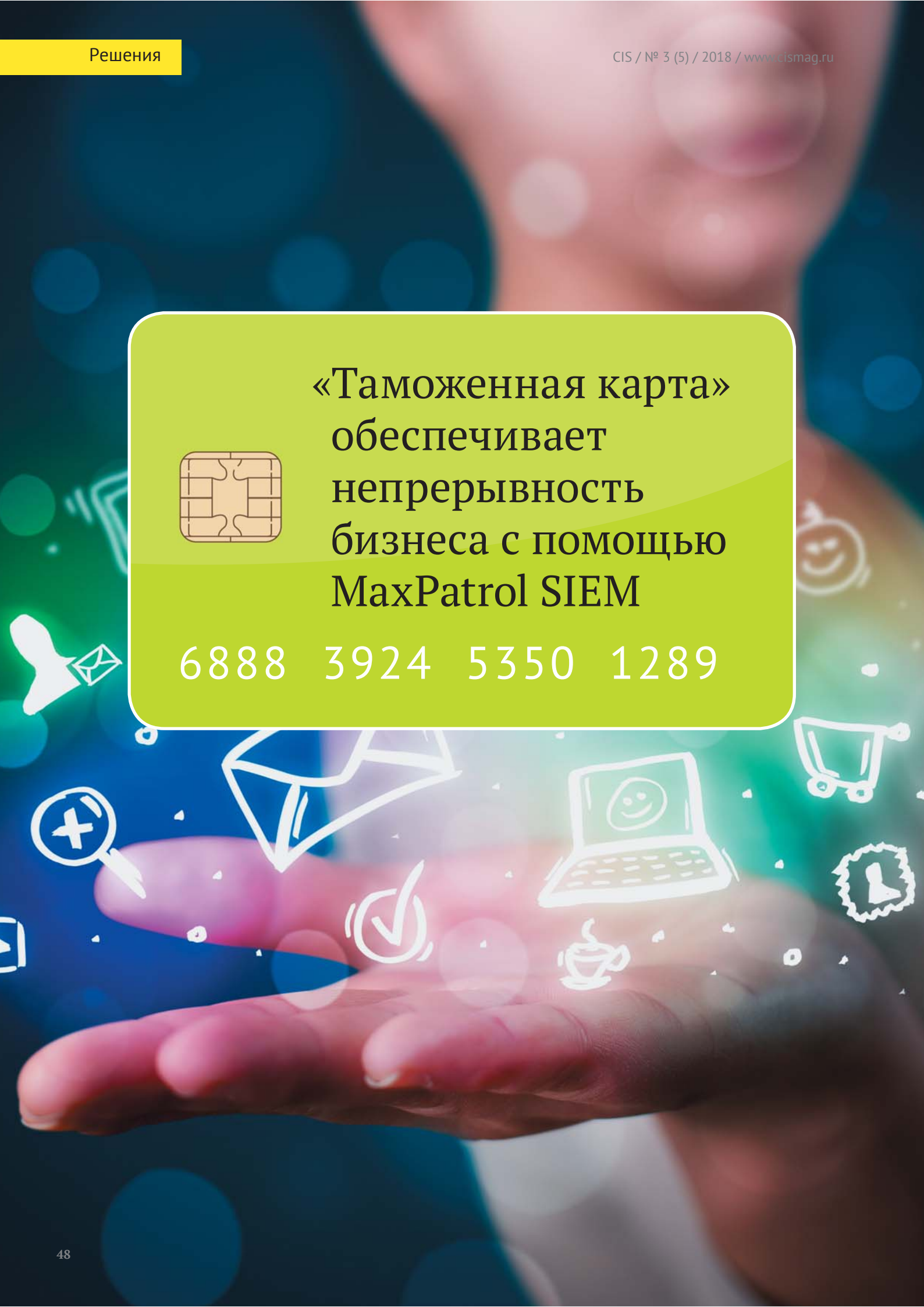
UserGate обеспечивает и применение ряда мер безопасности для публичных и частных сетей Wi-Fi. С помощью UserGate можно аутентифицировать пользователей самыми различными способами, применять к ним определённые политики безопасности, контролировать доступ к тем или иным ресурсам, блокировать загрузку опасного и запрещённого содержимого. Все эти меры позволяют значительно повысить безопасность интернет-доступа, а также обеспечить выполнение требований законодательства и/или внутренних регламентов компании.

UserGate

ООО «Юзергейт»
является удобной в управлении и доступной альтернативой зарубежным программным и аппаратным решениям, обеспечивающим безопасность доступа в интернет, защиту от внешних атак и контроль трафика.

www.usergate.ru

www.usergate.com



«Таможенная карта» обеспечивает непрерывность бизнеса с помощью MaxPatrol SIEM

6888 3924 5350 1289

Платёжная система «Таможенная карта» отслеживает события безопасности и выявляет инциденты при помощи MaxPatrol SIEM LE. В результате служба ИБ компании может получать полную информацию об инфраструктуре в любой момент, автоматически выявлять проблемные и новые активы, аномалии, подозрительные активности в инфраструктуре. Это помогает обеспечить непрерывность бизнеса компании в соответствии с установленным SLA: все виды финансовых операций проводятся в любом таможенном органе на территории России в режиме 24/7.

Основная задача «Таможенной карты» – совершенствование системы уплаты таможенных платежей и сокращение сроков таможенного оформления товаров. На сегодняшний день в числе участников платёжной системы более семидесяти государственных и частных банков и более шестидесяти таможен. Ежемесячный объём денежного оборота платёжной системы составляет от 50 до 70 млрд руб. Поэтому вопросам непрерывности бизнеса и надёжности финансовых транзакций уделяется первостепенное значение, в том числе с точки зрения информационной безопасности.

До внедрения SIEM-системы анализ событий безопасности в «Таможенной карте» проводился вручную, что не позволяло оперативно реагировать на обнаруженные угрозы. Конфигурации сетевых узлов регулярно меняются (практика Positive Technologies показывает, что в течение года инфраструктура любой организации обновляется в среднем на треть), и отсутствие актуальных знаний об инфраструктуре мешало выявлять инциденты. Поэтому для автоматизации анализа событий ИБ и выявления атак, аномалий и подозрительных действий в инфраструктуре было принято решение внедрить SIEM-систему.

Департамент информационной безопасности компании оценил возможности трёх самых популярных систем в России – IBM QRadar, ArcSight и MaxPatrol SIEM. Сравнивались возможности интеграции и взаимодействия с инфраструктурой, а также ценовая политика. По итогам тестирования «Таможенная карта» выбрала SIEM-систему компании Positive Technologies версии LE – как наиболее соответствующую всем заявленным требованиям:

- законченное коробочное решение для небольших инфраструктур (общее количество сетевых узлов в «Таможенной карте» – 200);
- дополнительные источники событий подключаются бесплатно в рамках техподдержки;
- доступная цена;
- присутствие в реестре отечественного ПО.

Подразделение ИБ самостоятельно внедрило и настроило MaxPatrol SIEM LE. Весь проект занял три месяца. За это время к SIEM-системе были подключены рабочие станции и источники с наибольшим количеством событий – контроллеры домена, прокси-серверы и межсетевой экран (всего около 100 узлов). Сегодня к источникам событий добавились инфраструктурные серверы, системы защиты, бизнес-системы и критически значимые файловые серверы. На основе поступающих из источников данных MaxPatrol SIEM LE формирует базу активов и по правилам корреляции выявляет инциденты. По итогам пилота «Таможенная карта» получила полностью работающий инструмент, готовый к промышленной эксплуатации.

«MaxPatrol SIEM LE – это быстрый способ получить работающую SIEM-систему,» – комментирует Сергей Горчаков, директор по ИБ «Таможенной карты». За три месяца с помощью консультаций специалистов Positive Technologies нам самостоятельно удалось внедрить систему и настроить необходимые источники. Благодаря этому мы получили подробную картину ИТ-инфраструктуры и отслеживаем инциденты ИБ. В дальнейших планах подключение к источникам событий серверов собственного удостоверяющего центра».

Функциональность MaxPatrol SIEM LE регулярно расширяется. Так, начиная с версии 4.0, в продукт автоматически поставляются знания экспертного центра безопасности Positive Technologies, что позволяет ему эффективно противодействовать новым типам угроз. Знания поставляются в виде пакетов экспертизы, которые содержат правила корреляции по выявлению инцидентов, актуальные правила нормализации и агрегации, рекомендации по тонкой настройке аудита на источниках событий и по расследованию. Выход экспертных пакетов запланирован не реже одного раза в два месяца.

POSITIVE TECHNOLOGIES

Positive Technologies *— один из лидеров европейского рынка систем анализа защищённости и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени.*

Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

www.ptsecurity.com

Таможенная Карта
Платежная система

Платежная система «Таможенная карта» *— оператор таможенных платежей № 1 в России. Компания «Таможенная карта» занимается развитием системы расчётов на основе технологии, утверждённой Приказом № 757 от 3 августа 2001 года, зарегистрированным в Минюсте России за № 2865 от 10 августа 2001 г.*

В соответствии с генеральным соглашением с ГТК России компания «Таможенная карта» имеет право на предоставление права эмиссии коммерческим банкам РФ и обеспечение проведения расчётов по таможенным платежам, проведённым с использованием таможенных карт. Среди клиентов «Таможенной карты» ведущие предприятия пищевой промышленности, авиаперевозчики, предприятия нефтяного и энергетического комплекса, импортёры медикаментов, лесоперерабатывающие предприятия.

Календарь мероприятий

20 сентября
Харьков • Митап
Съесть собаку #14: PHP

20 сентября
Санкт-Петербург • Мастер-класс
Мотивация и профессиональное выгорание в команде разработки

21 - 22 сентября
Минск • Конференция
CSS-Minsk-JS 2018

21 - 22 сентября
Киев • Конференция
Agile Rock Conference 2018

21 сентября
Минск • Мастер-класс
Workshop: Digital Маркетинг. Экспресс-погружение

22 сентября
Новосибирск • Конференция
MobiFest

22 сентября
Минск • Конференция
EPAM Software Engineering Conference: Make it Real

22 - 23 сентября
Казань • Хакатон
Digital SuperHero HackDays

22 сентября
Санкт-Петербург • Турнир
Турнир по кикеру «IT»s KICKER #5»

22 - 23 сентября
Москва • Курс
Профессиональный курс веб-аналитика

22 - 29 сентября
Афины • Тренинг
Первые. Релиз 2018

22 сентября
Винница • Митап
Vinnytsia Backend Meetup

24 сентября
Онлайн-трансляция • Вебинар
Как настраивать рекламу в контекстно-медийной сети Google Ads в Казахстане

24 сентября - 14 декабря
Санкт-Петербург • Курс
Veeam Academy: вечерний бесплатный интенсив «Программирование на C#»

25 сентября
Новосибирск • Тренинг
Семинар о TrueConf Server 4.4 и новинках AV-оборудования в Новосибирске

25 сентября
Москва • Конференция
Конференция «Интернет вещей»

25 сентября
Москва • Конференция
International Blockchain Summit Moscow

25 сентября
Москва • Конференция
Технологии машинного обучения

25 сентября
Онлайн-трансляция • Мастер-класс
Источники бесплатного трафика для вебинаров

25 сентября - 1 ноября
Минск • Курс
Основы UI/UX дизайна #пользователи #дизайн-системы #прототипирование

25 сентября - 25 марта
Москва • Курс
Java Junior программист (android-developer)

27 сентября
Онлайн-трансляция • Вебинар
Информационные запросы: разыскиваем трафик для вашего сайта

27 сентября
Минск • Митап
Salesforce Meetup Commerce Cloud and Marketing Cloud

27 сентября
Баку • Конференция
Blockchain & Bitcoin Conference Baku

27 сентября
Екатеринбург • Онлайн-трансляция • Конференция
Код ИБ Екатеринбург

27 сентября
Красноярск • Тренинг
Семинар о TrueConf Server 4.4 и новинках AV-оборудования в Красноярске

27 сентября - 27 января
Москва • Курс
Разработчик игр (Unity 3D)

28 сентября
Минск • Конференция
GoWayFest 2.0

28 - 29 сентября
Киев • Тренинг
Data Science и машинное обучение для бизнес-аналитиков

28 сентября
Москва • Конференция
MBLT DEV 2018

28 сентября - 29 октября
Москва • Курс
Копирайтинг (Написание продающих текстов)

28 сентября - 28 октября
Санкт-Петербург • Онлайн-трансляция • Курс
Курс UX-Дизайнер. Быстрый старт в профессию

28 сентября - 22 октября
Минск • Курс
JS на практике: с нуля до Vue. js.

29 сентября - 23 декабря
Москва • Курс
Школа разработки интерфейсов Яндекса

29 сентября
Тольятти • Митап
Большой QA Panda-Meetup

29 сентября - 28 октября
Москва • Курс
Офлайн-интенсив Медиа дизайн

29 сентября
Амстердам • Конференция
Blockchain Day Netherlands

29 сентября - 29 января
Москва • Курс
3D моделирование (Autodesk 3ds Max)

29 сентября
Минск • Мастер-класс
Совместный мастер-класс для IT компаний и заказчиков IT проектов

30 сентября
Ульяновск • Конференция
РИФ. Технологии 2018

1 - 31 октября
Минск • Курс
Imaguru Blockchain School

1 октября - 10 ноября
Москва • Курс
Контент: от идеи до продвижения

1 - 12 октября
Онлайн-трансляция • Вебинар
Онлайн-курс: Основы Salesforce

2 - 3 октября
Москва • Конференция
Открытая конференция для бизнеса и ИТ 2018. Глобальный тур Терrасофт

4 октября
Москва • Конференция
ИКТ в страховании 2018

4 октября
Онлайн-трансляция • Конференция
What is UX? Международная онлайн-конференция UX-Марафон #13

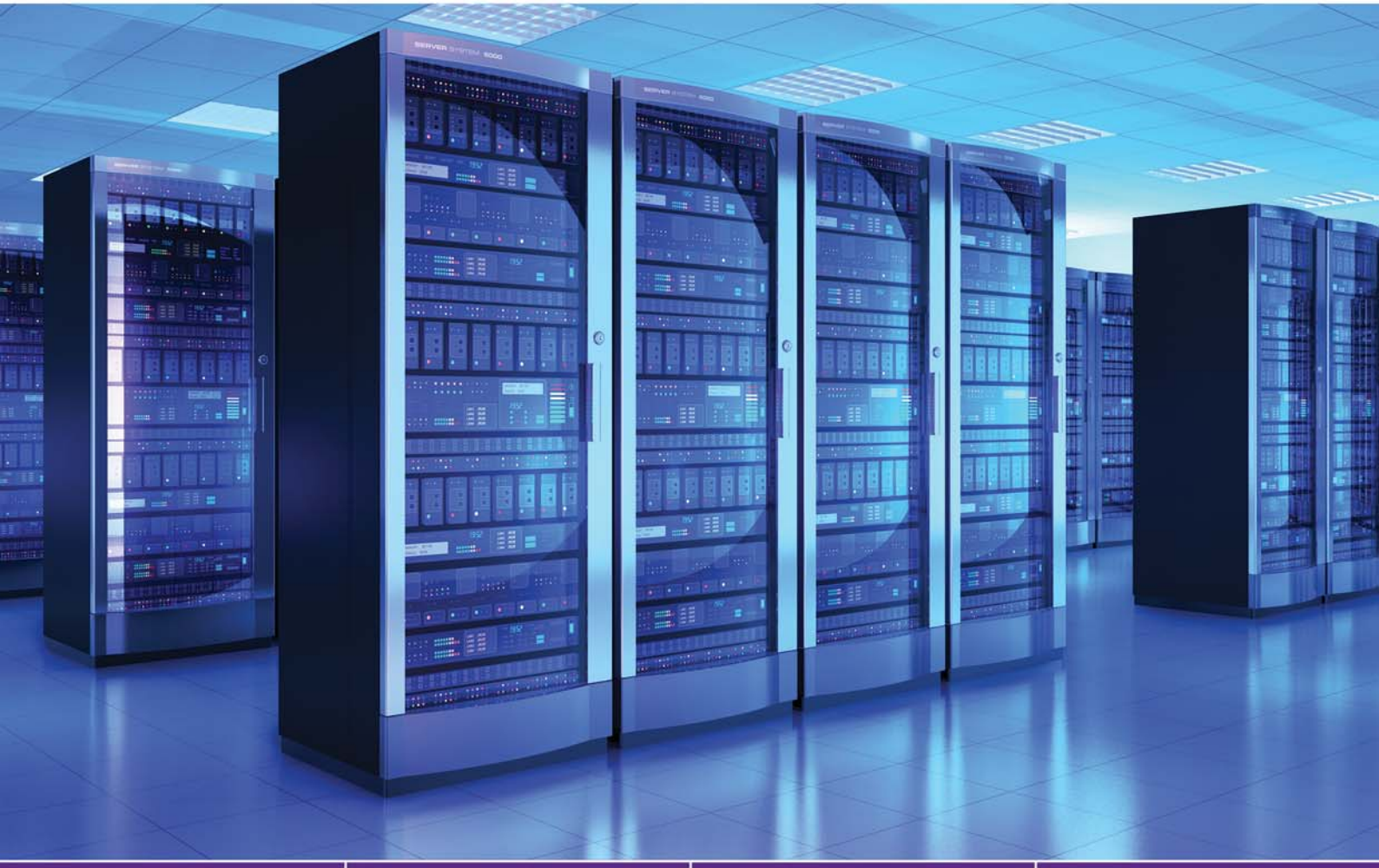
4 октября - 8 ноября
Онлайн-трансляция • Курс
Фундаментальный курс по SEO

5 - 7 октября
Санкт-Петербург • Хакатон
Хакатон Умный автомобиль

6 - 7 октября
Сочи, Россия • Конференция
Пионерский бизнес-лагерь «Перезагрузка». Как предпринимателям строить бизнес с грамотными удалёнными сотрудниками.

25 октября 2018
Москва • Конференция
IT-конференция по ИБ «CISummIT»

Лучшие в мире решения для информационной безопасности



Дистрибуция

Сертифицированные решения

Мобильные технологии

Канальное шифрование

TESSIS является официальным дистрибутором компаний Gemalto и CYREN, имеет статус Reseller у компании Blackberry и предлагает решения, обеспечивающие комплексную защиту и использующие технологии шифрования для защиты систем коммуникаций, программных разработок и контроля цифровой идентификации, а также решения для корпоративных и частных виртуальных сред.

TESSIS
TECHNOLOGIES, SYSTEMS AND SOLUTIONS FOR INFORMATION SECURITY

Научный проезд, 6, Москва
Тел.: +7 (495) 228-02-08
www.tessis.ru info@tessis.ru