CIS
Современные Информационные Системы
№ 4 (10) / 2019

Мисс CIS 2019

Стр. 48

Символ информационной безопасности России

«Актив»: 25 лет

Стр. 32

на рынке ИБ

ПРЕДИСЛОВИЕ

РЕШЕНИЯ

ПРОДУКТЫ

МЕРОПРИЯТИЯ

ОПЫТ

МИСС CIS

КУЛЬТУРА

ТЕХНОЛОГИИ

КРОССВОРД

КАЛЕНДАРЬ

От редактора

Дорогие читатели!

С гордостью представляем наш юбилейный – 10-й выпуск номера! Подводя итоги уходящего 2019 года, хотим отметить, что он оказался невероятно насыщенным и ознаменовался для журнала рядом важных событий.

В течение года мы успели примерить на себя и роль участника, и спонсора, и организатора ИТ-мероприятий.

Редакция приняла участие в организации и проведении такого крупного и знакового мероприятия в России как «РусКрипто». Журнал поддержал студентов, выступивших в рамках секции «Дни ВУЗов», и опубликовал их доклады.

Мы выступили в качестве информационного партнёра Skolkovo Cybersecurity Challenge – одного из самых престижных и значимых международных конкурсов инновационных проектов, направленных на защиту мира от киберугроз.

Организовали благотворительную конференцию CISummIT Digital Hearts и собрали средства в поддержку Благотворительного Фонда Константина Хабенского. Доклады с этого мероприятия ищите на страницах юбилейного номера журнала.

И конечно, нельзя не упомянуть о ежегодном всероссийском конкурсе красоты «Мисс CIS» 2019 среди девушек, работающих в ИТ-сфере. С подробностями этого феерического шоу и статьями участниц конкурса вы можете ознакомиться уже в этом выпуске.

Продолжая традицию дарить подарки под Новый Год, мы подготовили для вас большой красивый календарь. Просто напишите запрос на почту info@sovinfosystems.ru, и вам его обязательно доставят.

Редакция журнала CIS от души поздравляет вас с Новым 2020 Годом! Пусть в наступающем году Белой Крысы каждый из вас получит тот заветный кусочек сыра, о котором втайне мечтает уже много лет. С Новым годом вас, друзья! Счастья, понимания и любви!

С уважением,
редакция журнала CIS.

Главный редактор: Станислав Понарин.

Корректор: Оксана Макаренко.

Отдел рекламы и распространения: info@sovinfosystems.ru.

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

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

Номер свидетельства: ПИ № ФС 77-69584.

Дата регистрации: 02.05.2017.

Наименование СМИ: Современные Информационные Системы.

Форма распространения: печатное СМИ, журнал.

Территория распространения: Российская Федерация.

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

Язык: русский.

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

Фото на обложке: Анастасия Колоскова.

Тираж 5000 экз. (отпечатанный тираж).

Журнал предназначен для лиц старше 16 лет.

Дмитрий Петерсон,
операционный директор
SimbirSoft

Мобильное приложение: 5 шагов для выбора разработчика

Мобильный канал коммуникаций приобретает всё большее значение для бизнеса. Мы в mobile.SimbirSoft помогаем компаниям улучшить их приложения или создать с нуля. Предлагаем алгоритм, который поможет найти подрядчика и избежать ошибок.

Рынок мобильных приложений продолжает стремительно расти. В 2018 году пользователи App Store и Google Play загрузили различные приложения и игры 113 миллиардов раз, потратив $76 млрд, что на 10% и 20% соответственно выше прошлогоднего результата, по оценкам App Annie.

Пользователи проводят в приложениях более 3 часов ежедневно, и с каждым годом на 10% больше. При этом не все приложения, как и не все стартапы, успешны. Согласно *отчёту CB Insights 2017 года*, до 70% технологических стартапов проваливаются по тем или иным причинам, например из-за отсутствия рыночной потребности или недостатка средств на развитие.

Для того чтобы снизить риски разработки, бизнес обращается в ИТ-компании за услугами аутсорсинга. За счёт своей экспертизы и ресурсов правильно выбранный аутсорсер может спрогнозировать и устранить большинство рисков.

Путь к выбору исполнителя

Следующие советы предназначены для тех компаний, которые уже обозначили свою бизнес-задачу и находятся в поиске исполнителя. Если сначала нужно определить бюджет проекта, найдите подходящие приложения и обратитесь за оценкой к их мобильным разработчикам.

Так вы найдёте компании с релевантным опытом и уже во время первых переговоров сможете узнать, на какой минимальный бюджет разработки следует рассчитывать.

Шаг первый. Определение кандидатов

Выбрать мобильных разработчиков вы можете с помощью следующих источников:

- публикации кейсов мобильных разработчиков;
- рекомендации ваших знакомых;
- деловые контакты, полученные на профильных выставках;
- личные контакты мобильных студий.

Изучите деятельность каждой выбранной компании. Зайдите на сайт, посмотрите портфолио, постарайтесь оценить масштаб работ компании. Найдите группу компании в социальных сетях или профили её руководителей, чтобы убедиться в том, что это действующий участник рынка.

Важные критерии оценки:

- наличие у компании рекомендаций от коллег в вашей сфере бизнеса;
- наличие релевантного или схожего по масштабу опыта;
- свидетельства практической деятельности компании, наличие актуальных новостей в социальных сетях;
- зрелость компании.

Если вы потенциально готовы работать с компанией, внесите её название и контактные данные в отчёт. После этого вы можете отправить свой запрос в каждую из компаний-участников.

Шаг второй. Сбор коммерческих предложений

Успех реализации вашего проекта зависит от того, насколько эффективно пройдёт сбор коммерческих предложений. Здесь важно оценить ресурсы каждого разработчика и предоставить всем единые данные о планируемом проекте.

Если все участники по-разному представят себе реализацию ваших идей,

то в результате вы получите совершенно разные цифры. При этом высокая стоимость услуг не гарантирует, что проект не выйдет за пределы планируемого бюджета после учёта всех особенностей вашей идеи. Точно так же низкая стоимость услуг сама по себе не является показателем риска, она не означает, что оценка занижена или что при разработке проекта возникнут те или иные проблемы.

Участники конкурса могут по-своему представлять состав работ и выбирать различные технологии реализации. Например, **кто-то может предложить нативную разработку мобильных приложений, а кто-то – кроссплатформенную**. Каждый разработчик предложит свою стоимость услуг, каждый вариант будет иметь свои плюсы и минусы, которые определяются используемыми технологиями.

Бывают случаи, когда к заказчику приходят новые идеи по проекту уже после того, как он отправил разработчикам свои запросы. В этом случае все уточнения и идеи необходимо снова разослать всем участникам. Это позволит корректировать аутсорсерам свои предложения: они будут более релевантны, что впоследствии уменьшит вероятность спорных или конфликтных моментов.

Шаг третий. Проведение переговоров

После отправки запросов вы переходите к следующему этапу – проведению переговоров и митингов с разработчиками. Команды будут презентовать себя и задавать вопросы. Ваша цель – определить, какие компании обладают собственными ресурсами для выполнения вашего проекта, а какие делегируют задачи своим подрядчикам.

Задайте несколько вопросов, чтобы свести к минимуму основные риски.

1. Есть ли у компании собственный штат разработчиков? Привлекает ли она к своим проектам субподрядчиков или фрилансеров?
Важно определить соотношение собственных и приглашённых специалистов на данный момент. Если внешних разработчиков больше, очевидно, что мобильная студия не разрешит возможные проблемы подрядчиков своими силами.

2. Готова ли компания предоставить доступ к таск-трекеру проекта?
Чем более прозрачно идёт работа, тем меньше риск провала. Имея доступ к таск-трекеру, вы сразу видите, кто из специалистов работает над задачами, как быстро эти задачи закрываются, сколько осталось до конца проекта т. п. В случае проблем вы распознаете их на гораздо более ранних сроках.

3. Готова ли компания подключить вас к командным митингам?
Вам не обязательно участвовать в них ежедневно. Однако возможность подключиться и пообщаться с командой имеет большое значение (и исключает вероятность «подмены» специалистов, если вы общаетесь с помощью видео).

4. Предоставляет ли компания исходный код в виде репозитория?
Если впоследствии над проектом будут работать другие исполнители, это сделает их работу проще.

5. Имеет ли компания на данный момент свободные ресурсы для реализации вашего проекта?
Проблемы нет, если вы можете подождать. А если задача очень срочная, то следует оценить именно те ресурсы, которые свободны в данный момент, а не появятся «в ближайшую неделю». Как показывает практика, этап завершения текущих проектов может затянуться, например в связи с реализацией дополнительных пожеланий клиентов.

6. Будет ли компания сама делать все компоненты вашего проекта (сервер, CMS, мобильные и веб-клиенты)? Или для этого будет привлечён другой партнёр?
Уча стие другого партнёра – это риск, даже если компания ранее успешно реализовала подобные проекты с участием тех или иных подрядчиков.

Шаг четвёртый. Фильтрация коммерческих предложений

После того, как вы получили достаточный объём предложений и провели начальные переговоры, можно приступать к фильтрации участников конкурса.

В первую очередь исключите компании, которые имеют критерии риска. Например:

- сокрытие информации о команде разработчиков;
- отсутствие доступа к таск-трекеру и митингам;
- есть сомнения в компетенции компании и др.

Не выбирайте команду с рисковыми параметрами только по той причине, что вам понравилось с ними общаться. Не стоит обманываться, что в вашем случае всё будет хорошо.

На этом этапе желательно оставить не больше 2-3 потенциальных исполнителей. Прочим участникам предложите составить примерный план работ (дорожную карту) по проекту и потом провести митинг с той командой, которая будет заниматься разработкой. С помощью дорожной карты вы и исполнитель сможете спланировать работы и необходимые ресурсы. А с помощью общения с потенциальной командой вы поймёте компетенцию специалистов и повысите вероятность успеха проекта.

Если отдельные компоненты системы будет делать не основной подрядчик, а другие исполнители, желательно их тоже пригласить на обсуждение.

Шаг пятый. Принятие решения

На финальном этапе выбора мобильного разработчика всё просто: вам нужно принять решение. Естественно, на него могут влиять различные факторы, в том числе сроки и бюджет разработки, подход команды к работе, общие впечатления от общения. Оцените всю информацию и потенциальные риски.

В случае мобильной разработки (фронтовой части) наибольший вес имеют такие параметры, как связка ресурсов и способностей компании. При этом вам должно быть комфортно на равных общаться с исполнителем.

Выводы

Несмотря на большое число потенциальных исполнителей, на практике оказывается непросто найти надёжную команду, способную без проблем решить вашу задачу. Для этого есть много причин как со стороны клиента, так и со стороны исполнителя. Вложите в процесс выбора достаточное количество труда и времени, и впоследствии ваши усилия не раз окупятся. Не дайте себя обмануть красивыми словами: смотрите только на цифры и результаты.

---

mobile.SimbirSoft

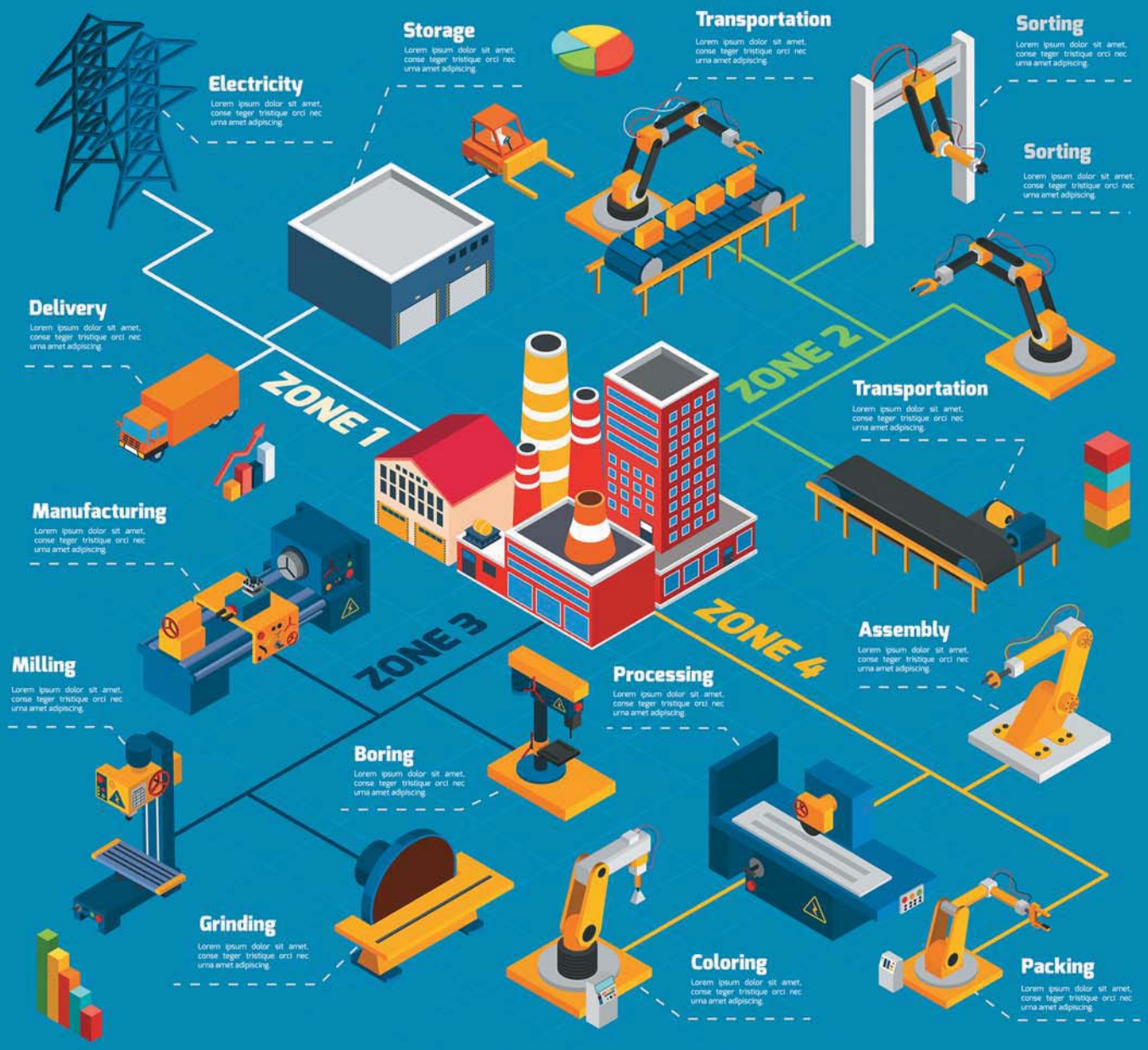
mobile. SimbirSoft *– с 2008 года создает мобильные приложения для бизнеса, для финтеха, ритейла, телекоммуникационных и сервисных компаний.*

mobile.simbirsoft.ru

Цифровая трансформация управления производством

Компания «ЕАЕ-Консалт» продолжает внедрение собственной информационной системы управления производством DigitalPlant («Цифровой завод») на одном из отечественных предприятий. В основу решения положена цифровая модель предприятия – краеугольный камень современной MES.

Новое решение включает в себя уникальные модули календарного планирования и сведения материального баланса, разработанные в соавторстве с учёными МГУ. Система управления производством охватывает весь периметр предприятия от технологических установок до отгрузки. Завершение проекта ожидается в конце первого квартала 2020 года.



Информация о системе

Комплексная MES-система управления производственными процессами DigitalPlant предназначена для оперативного управления производственной деятельностью предприятия непрерывного цикла и интегрируется с системами нижнего (АСУ ТП) и верхнего (ERP) уровней.

Функциональные возможности системы обеспечивают сбор информации о материальных потоках за определённые интервалы времени (месяц, неделя, сутки); точный учёт компонентов и готовых продуктов; планирование, учёт и контроль движения продукции; прогнозирование развития ситуации с учётом технологических ограничений; автоматизированный расчёт материального баланса; расчёт неизмеримых потоков и согласование противоречивых измерений.

Решение DigitalPlant

Приступая к проекту создания собственной системы уровня MES, мы внимательно изучили предлагаемые решения и пришли к выводу, что на рынке нет готового продукта, удовлетворяющего целям современного предприятия. Поэтому для оперативного управления производством была разработана собственная система DigitalPlant (рис. 1), которая обеспечит решение целого комплекса задач:

- **календарное планирование:** контроль за деятельностью предприятия в режиме, близком к режиму реального времени, с прогнозированием развития ситуации на любом временно́м горизонте;
- **диспетчерское управление:** регистрация и контроль исполнения распоряжений;
- **моделирование производства:** актуализация модели предприятия;
- **сбор производственных данных** с минимальным влиянием человеческого фактора;
- **расчёт движения продукции и сведение материальных балансов** на основе данных средств измерений;
- **план-факт анализ:** ежедневный контроль достижимости целей экономического плана.

Основной задачей системы является контроль исполнения оптимального экономического плана предприятия.

Взаимодействие модулей

Все подсистемы опираются на единую цифровую модель предприятия. Любая плановая операция, производственное задание, технологическое событие или отчёт связаны с объектом модели: потоком, технологической установкой, резервуаром. Такой подход позволяет легко собрать данные о фактическом состоянии производства из разных подсистем и сопоставить их с плановыми показателями.

Календарное планирование

а) планирование выработки

Календарное планирование является важнейшей частью автоматизации предприятия, позволяющее создавать проект календарного плана выработки товарной продукции на основе экономического плана предприятия.

В нашей системе процесс КП разделён на две части: расчёт КП для непрерывного производства (например установки) и дискретный (например резервуары). Эти части лучше рассматривать отдельно и реализовывать КП тремя этапами.

Сергей БАЛАШОВ,
начальник Управления производственных систем бизнес-сегмента «Переработка и Сбыт» ООО «ЕАЕ-Консалт»

Рисунок 1. Структура информационной системы DigitalPlant.

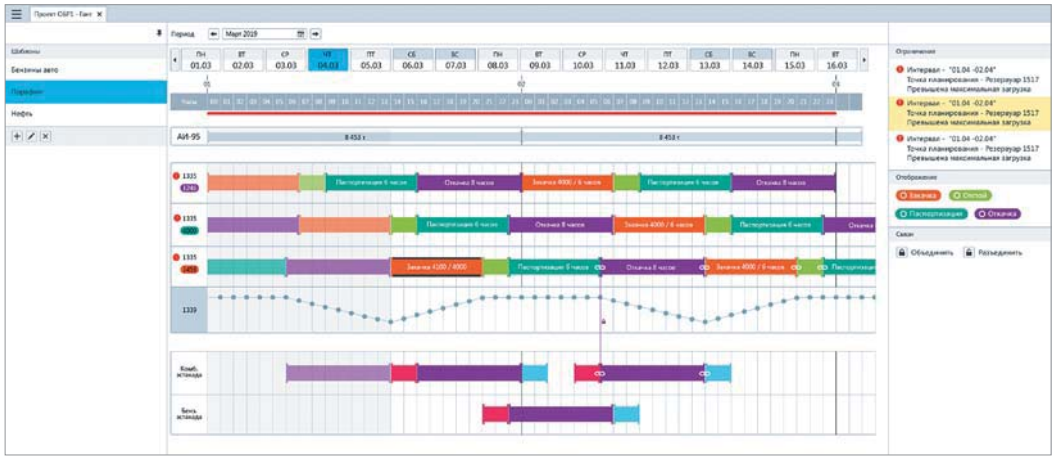


Рисунок 2. Календарное планирование: резервуары и эстакады.

Первый этап – планирование получения готовой продукции. Мы даём возможность загрузить экономический план и равномерно распределяем его на месяц, что даёт нам очень приблизительный календарный план. Главное на этом этапе – получить ориентиры: сколько и какой продукции надо выработать за месяц.

Дальше пользователь может его скорректировать. Например, необходимо выработать 600т продукта N. При первичном распределении эти 600т программа распределяет по 20т на весь месяц. Но 600т – это всего 3 дня работы установки, делать весь месяц по 20т мы не можем. Пользователь выбирает период, в котором хочет выработать это количество, и программа автоматически пересчитывает календарный план. В нашем случае в тех периодах, в которых продукт N вырабатываться не будет, увеличивается выработка других продуктов. Таким образом, суммарно за месяц прогноз по выработке каждого вида продукта не изменился и остался равен значениям, полученным из экономического плана.

б) резервуары/эстакады

На *втором этапе*, зная, когда и сколько будет выработано продукции, мы должны распределить её по резервуарам.

На рисунке 2 сверху – ресурс продукта N. Программа последовательно, согласно настроенному шаблону, заполняет 1-й резервуар. Поступление в него – это оранжевая полоса. Далее за ней следует светло-зелёная – это период отстоя, и бирюзовая – это паспортизация. Сиреневым выделено время, когда в резервуаре есть нужное количество продукта. Потом алгоритм создаёт такие же шаблонные операции для следующего резервуара, совмещая начало поступления в него с окончанием загрузки в 1-й. Таким образом распределяется весь запланированный к выработке ресурс. И, что самое важное, определяются интервалы времени, когда в резервуарах будет нужное для отгрузки количество продукта.

Затем необходимо спланировать отгрузку этих продуктов. Здесь весь планируемый период просто заполняется шаблонными операциями, состоящими из подачи вагонов (красная полоса), загрузки (сиреневая), уборки (голубая). За счёт этого в первом приближении обеспечивается непрерывная нагрузка эстакады.

После этого остаётся только установить связь между операцией загрузки на эстакаде и отгрузки из резервуара. Любое изменение в плановых операциях приводит к их пересчёту. График показывает изменение остатка в резервуаре, при этом в прошлом виден факт, а в будущем – прогноз.

в) производство

На *третьем этапе*, после того как определено, какой должна быть выработка, мы должны выдать производственные задания на установки, и здесь в дело вступает наука. Совместно с сотрудниками факультета вычислительной математики и кибернетики МГУ разработан новый, адаптированный под задачу КП, математический метод, позволяющий составить такое расписание из заранее определённых режимов работы установок, которое позволит при существующих технологических ограничениях выработать запланированное количество продукта. Метод очень сложный, но суть проста: мы выбираем из набора режимов работы установок такие, которые позволяют выработать нужные продукты, и рассчитываем время, когда надо перейти с одного на другой.

Сбор производственных данных

Подсистема в терминах цифровой модели аккумулирует все сведения о работе предприятия, опираясь на доступные источники данных: единую базу данных реального времени (БДРВ), лабораторную систему (ЛИМС), РСУ, данные ручного ввода. Включает в себя сервер технологических расчётов, реализующий стандартизированные методики расчёта масс, и аппаратно-математические измерители, которые позволяют рассчитывать массу на любом потоке, резервуаре жидкости или газа.

Моделирование

Среди оригинальных решений, разработанных нами в ходе проекта, – создание единой информационной модели предприятия, которая позволяет формировать направленный

граф материальных потоков, системы ограничений и модели материальных потоков предприятия за балансовый период, создавать сложные расчётные измерители.

Согласование материального баланса

В основе системы согласования матбаланса лежит инновационная разработка – алгоритм нахождения оптимального решения системы линейных уравнений (оптимальность понимается в смысле наибольшего соответствия измеренным значениям), созданный также совместно с учёными МГУ, который отличается от общепринятых двумя важнейшими преимуществами.

Во-первых, мы решаем задачу согласования баланса с учётом технологических ограничений. Это усложняет алгоритмы решения, но позволяет получить достоверный результат.

Во-вторых, наше решение выдаёт по-настоящему целочисленный результат. Кроме того, разработанные для решения задачи математические методы активно развиваются.

Ядро подсистемы – **математическая модель (решатель) производственных потоков**, разработанная совместно с учёными факультета вычислительной математики и кибернетики МГУ:

- используется как в составе комплексной MES-системы, так и в качестве самостоятельного программного обеспечения
- является мультиотраслевым решением
- превосходит существующие решения по скорости сходимости и точности сведения баланса (согласованные значения отклоняются от измеренных аналогов **минимально**).

Экономический эффект

Экономический эффект внедрения системы DigitalPlant можно рассчитать по многим параметрам, и он будет исчисляться сотнями миллионов рублей: оптимизация производственного цикла, отгрузки, запасов, увеличение выработки продукции и повышение её качества, выявление потерь. Для каждого предприятия это будут свои показатели.

Преимущества DigitalPlant

Благодаря внедрению системы DigitalPlant клиенты компании «ЕАЕ-Консалт» получают значительные конкурентные преимущества, среди которых отмечу основные.

1. *Внедрение DigitalPlant обеспечивает максимально возможный уровень автоматизации* процессов сбора, обработки, накопления, хранения и отображения информации о фактической работе объектов предприятия. Влияние человеческого фактора снижено до минимума. Одновременно мы не только определяем величину неизмеримых потоков, но и определяем потоки с низкой достоверностью и даём рекомендации по дооснащению производства средствами измерений.
2. *Все результаты деятельности предприятия могут быть спрогнозированы* за счёт моделирования действий по управлению производством.
3. *Автоматизирован бизнес-процесс расчёта материального баланса,* срок согласования баланса максимально сокращён.
4. *Автоматизированы процессы выдачи и контроля производственных заданий,* оперативно и в установленный срок формируется производственная отчётность, которая предоставляется по любой единице (установка, группы установок или завод) на любом горизонте планирования в привычных офисных форматах.
5. *Достигнут оптимальный режим функционирования производственных мощностей* за счёт оперативного получения достоверной информации об их работе.
6. *Возросла точность идентификации мест и причин возникновения потерь* за счёт определения ошибок, допущенных в ходе согласования баланса.
7. *Ведётся учёт движения материальных потоков (сырья, полуфабрикатов, готовой продукции).* DigitalPlant позволяет вести глобальный учёт цепочки поставок сырья и готовой продукции, оптимизировать процессы переработки, сводить к минимуму потери, связанные с отклонением от плановых заданий.
8. В отличие от большинства MES, подсистема план-факт анализа DigitalPlant осуществляет ОПЕРАТИВНЫЙ КОНТРОЛЬ ВЫПОЛНЕНИЯ календарного производственного плана и прогнозирование исполнения экономического плана предприятия, что позволяет обеспечить руководителей всех уровней оперативной информацией о выполнении или необходимости корректировки плановых показателей.

В результате осуществляется реальный переход работы предприятий от формата «по факту», т.е. по итогам оценки полученного результата с последующим принятием решений, к работе «по плану» – с максимально достоверным прогнозированием результатов и принятием обоснованных решений.

еае-консалт
Группа компаний ЭнСи

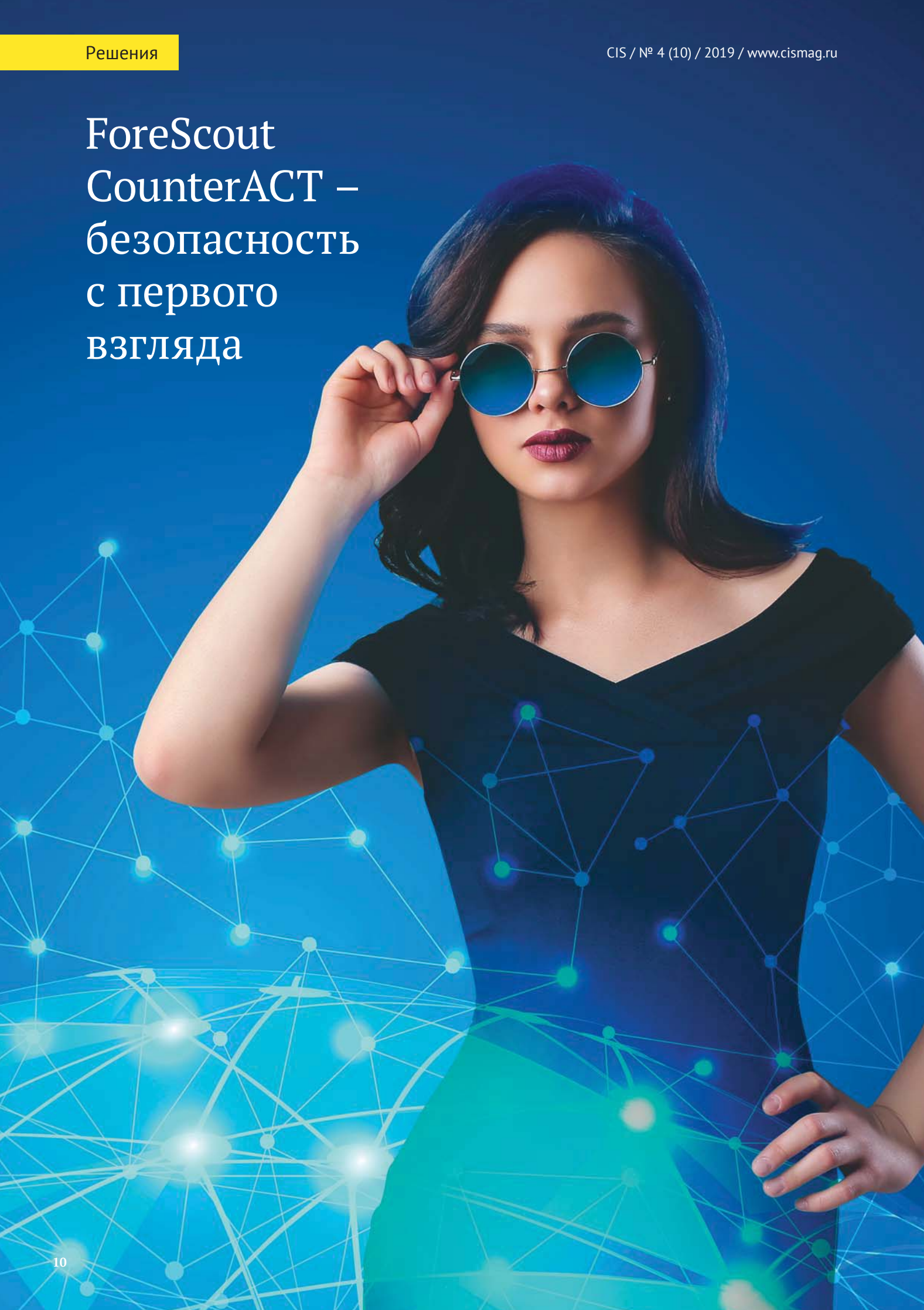
ООО «ЕАЕ-Консалт»

Тел.: +7 (495) 213-11-76

www.eae-consult.ru

info@eaeconsult.ru

ForeScout CounterACT – безопасность с первого взгляда



Безопасность начинается с понимания того, что находится внутри нашей сети. Ограниченная видимость приводит к появлению «слепых зон» безопасности. Большинство систем безопасности конечных точек требуют наличия на каждом устройстве современных агентов для их просмотра и управления.

Менеджеры ИТ-безопасности обычно не имеют представления о существовании неуправляемых конечных точек BYOD и растущем количестве устройств IoT, которые появляются в сетях каждый день и могут представлять угрозу для нашей сети. Это означает, что мы должны научиться автоматически производить идентификацию всех устройств в момент их подключения к сети, отслеживать их состояние на протяжении всего жизненного цикла в сети и быть способными оперативно реагировать на изменения состояния этих устройств.

Forescout Technologies является лидером в области видимости и контроля устройств. Единая платформа безопасности ForeScout позволяет предприятиям и государственным учреждениям получить полную ситуационную осведомлённость о своей корпоративной среде и организовать действия по снижению кибер и операционных рисков. Благодаря безагентскому подходу платформа Forescout быстро разворачивается, обнаруживает и классифицирует в реальном времени каждое устройство, подключённое к IP, а также непрерывно отслеживает состояние устройств на протяжении всего жизненного цикла устройства в сети.

Почему Forescout

- **Снижение рисков для бизнеса, связанных с нарушениями или инцидентами безопасности**
  Непрерывный контроль растущей сети предприятия для обнаружения, предотвращения и устранения несоответствующих устройств, которые угрожают безопасности и увеличивают затраты организаций.
- **Обеспечение и демонстрация соответствия требованиям безопасности**
  Непрерывная оценка безопасности вашей среды, чтобы убедиться, что каждое устройство соответствует вашей политики безопасности.
- **Повышение эффективности операций по обеспечению безопасности**
  Интегрируйте ForeScout с вашими существующими инструментами управления безопасностью и автоматизируйте процессы для повышения эффективности операций по обеспечению безопасности.

Что мы решаем?

Вчерашние подходы к безопасности требовали программных агентов, которые оказывались малополезными в случаях, когда нет возможности поставить агент на устройство или происходит отключение агента на конечной точке. Платформа Forescout быстро и безопасно развёртывается в гетерогенных кампусах, центрах обработки данных, облачных сетях и OT-сетях и позволяет решить следующие задачи без использования программных агентов:

- **Видимость устройств в сети**
  Вы не можете защитить то, что не видите™
  Непрерывное обнаружение, классификация и оценка каждого IP-устройства, подключённого к вашей корпоративной сети для унификации управления безопасностью.
- **Asset management**
  Защищайте и управляйте подключёнными точками
  Автоматизация процесса инвентаризации и поддержание всегда в актуальном состоянии информации обо всех ваших активах в ИТ и OT-сетях.
- **Device Compliance**
  Оценка и уверенность в Compliance
  Непрерывная оценка устройств, их контроль и применение политик безопасности для постоянного поддержания устройств в состоянии Compliance.
- **Управление доступом к сети (NAC)**
  Управление доступом – просто и легко
  Применение унифицированных политик NAC в гетерогенных кампусах, центрах обработки данных, облаках и средах OT как с 802.1x, так и без него.
- **Сегментация сети**
  Уверенная сегментация вашей сети
  Облегчённое планирование сегментации и автоматизация назначения ACL / VLAN для уменьшения поверхности атаки.
- **Реагирование на инциденты**
  Реагирование и оперативное устранение инцидентов
  Автоматизация обнаружения угроз, приоритезация и сдерживание для ускорения реагирования на инциденты и снижение рисков.

FORESCOUT

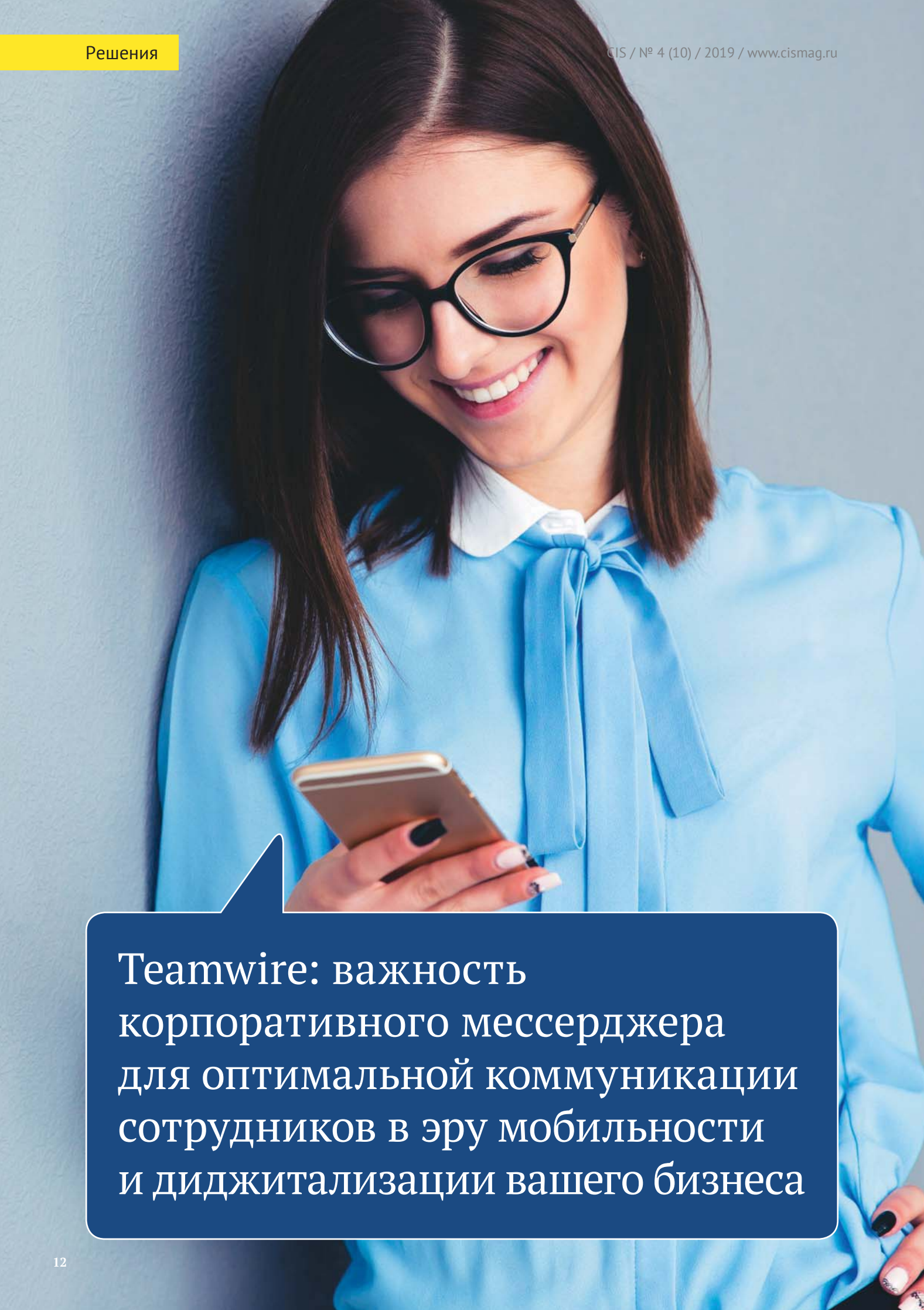
ForeScout CounterACT *– многолетний лидер магического Квадранта Gartner в сегменте Network Access Control за его способность видения.*

www.forescout.com | support@forescout.com

headtechnology
it-security distribution

HEADTECHNOLOGY Group *– специализированный дистрибутор, ориентированный на развивающиеся рынки Центральной и Восточной Европы, Балтии, стран СНГ и Центральной Азии.*

www.headtechnology.com | info@headtechnology.com



Teamwire: важность корпоративного мессерджера для оптимальной коммуникации сотрудников в эру мобильности и диджитализации вашего бизнеса

Мы находимся в эре мобильности и всё больше сотрудников различных компаний используют смартфоны и планшеты для своей повседневной работы.

Мобильность сотрудников – один из ключевых факторов продуктивности организаций. Именно использование мобильных устройств даёт возможность обеспечить совместную работу распределённых команд, коллег, клиентов и партнёров, в режиме реального времени – в офисе, в аэропорту, в командировке – всегда, когда это необходимо. Мобильные устройства позволяют получить удалённый доступ к корпоративным ресурсам, таким как документы и файлы, анализировать финансовые и производственные отчёты, обновлять данные клиентов в любое время и из любого места. И сегодня построение качественного и безопасного «мобильного офиса» критически важно для любой компании.

Обычно, на первом этапе ввода мобильности в организации, внедряются системы по управлению мобильности (MDM/EMM/UEM) для управления и защиты мобильных устройств при доступе к корпоративным ресурсам. После того, как мобильная инфраструктура защищена и управляется в масштабах всей компании, производительность конечных пользователей быстро становится ключевой темой и ведёт к дискуссии по следующим вопросам:

- К каким корпоративным ресурсам должен быть доступ у сотрудников с мобильных устройств?
- Какие рабочие процессы необходимо диджитализировать и как это можно сделать?
- Какие рабочие процессы могут быть ускорены с помощью мобильности?
- Какие инструменты нужны бизнесу для успешной работы мобильных и офисных сотрудников?
- Как обеспечить эффективную коммуникацию между сотрудниками?
- Какие приложения и сервисы должны стать частью «мобильного офиса»?

В результате для большинства предприятий, «мобильный офис» для смартфонов и планшетов состоит из электронной почты, PIM (контакты, календарь, заметки и т. д.), приложения для доступа/хранения/распространения файлов и корпоративный мессенджер. Почему организации определяют корпоративный мессенджер, как один из ключевых составляющих «мобильного офиса»:

- Оптимальный инструмент для командного общения и взаимодействия в режиме реального времени и быстрого принятия решений
- Простой в использовании, оптимизирован для мобильных устройств, обеспечивает неформальное общение, идеально подходит для групповых чатов и обеспечивает мгновенный обмен информацией по сравнению с электронной почтой
- Потребность безопасной замены «WhatsApp» и др. бесплатных мессенджеров, как части теневого ИТ, для обеспечения безопасности, защиты данных, администрирования и соответствия стандартам
- Потребность в инструменте, который обеспечит взаимодействие и обмен информацией между ПО, системами и службами организации – центральный информационный хаб бизнеса
- Диджитализация рабочих процессов путём подключения корпоративного мессенджера к ИТ-экосистеме организации для автоматического обмена информацией

Рынок корпоративных мессенджеров быстро развивается. На первый взгляд предложения поставщиков могут выглядеть одинаково, но, иметь существенный различия. Если вы ищете быстрое, интуитивно понятное и безопасное приложение для обмена корпоративными сообщениями для повышения производительности и улучшения взаимодействия вашей команды, стоит обратить внимание на Teamwire – лучшее немецкое решение в этом классе. А если у вас есть вопросы по этому направлению или вам бы хотелось протестировать решение в своей инфраструктуре, обращайтесь к нам за более подробной информацией.

TeamWire *– быстрое, интуитивно понятное и безопасное приложение для обмена корпоративными сообщениями.*

www.teamwire.eu

info@teamwire.eu

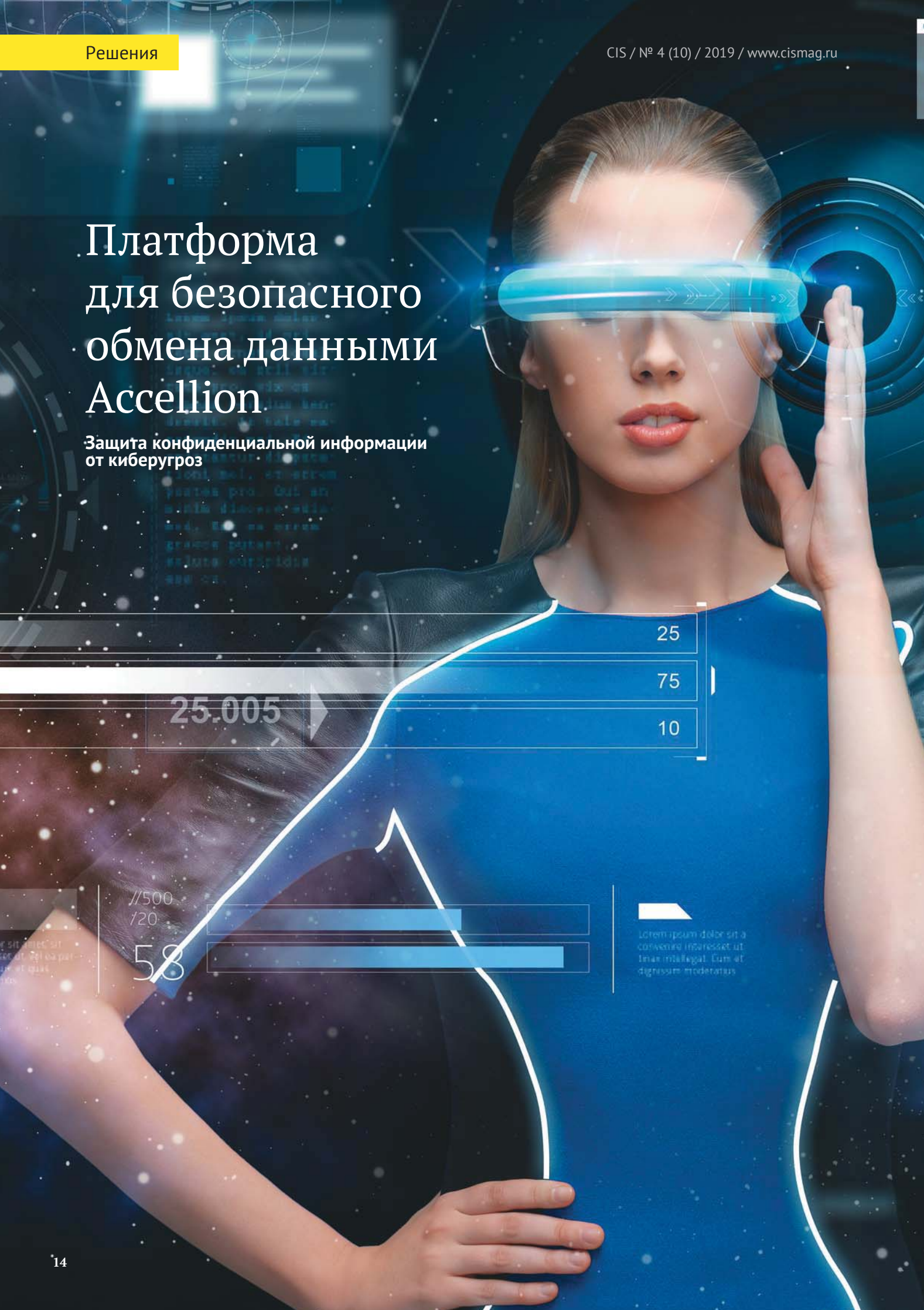
HEADTECHNOLOGY Group *– специализированный дистрибутор, ориентированный на развивающиеся рынки Центральной и Восточной Европы, Балтии, стран СНГ и Центральной Азии.*

www.headtechnology.com

info@headtechnology.com

Платформа для безопасного обмена данными Accellion

Защита конфиденциальной информации от киберугроз



Пролейте свет на внешние угрозы с помощью CISO Dashboard

Если вы когда-нибудь блуждали в тёмной комнате в поисках выключателя, то знаете, каково это – пытаться защитить конфиденциальные данные в организации. Если бы у вас был фонарик, то вы могли бы сразу же найти выключатель и не удариться рукой о стул в углу. CISO Dashboard – интерактивная обзорная панель, которая работает именно так, потому что она позволяет вам видеть все рабочие процессы, осуществляемые вашими сотрудниками для обмена конфиденциальной информацией с внешними партнёрами. В противном случае вы не сможете защитить то, чего не видите.

Полноценная защита должна охватывать весь спектр угроз: все входящие и исходящие каналы информации. Комплексная защита включает в себя мониторинг и управление всеми сторонними рабочими процессами, включая безопасную электронную почту, SFTP и обмен файлами.

Визуализация в режиме реального времени позволяет ответить на самые важные вопросы о безопасности персональных данных, интеллектуальной собственности и другой входящей и исходящей конфиденциальной информации.

Защитите чувствительную информацию от утечки и предотвратите внедрение вредоносного кода

Если ваш бизнес похож на большинство других, то он генерирует, собирает и передаёт конфиденциальные данные целый день, каждый день. Частная информация, такая как контракты, бюджетные прогнозы и данные о клиентах, часто передаётся доверенным третьим лицам: консультантам, юристам, бухгалтерам, поставщикам и прочим. К сожалению, всякий раз, когда вы делитесь этой информацией, то подвергаете себя многочисленным угрозам, включая вредоносные программы, фишинговые атаки и утечки данных. С помощью CISO Dashboard вы сможете наблюдать за активностями по передаче информации в вашей организации и обнаруживать аномалии, которые могли бы пропустить. Допустим, вы видите, как менеджер по маркетингу загружает финансовые отчёты и отправляет их кому-то с личной почты. Является ли это частью его рабочего процесса? Вы видите многочисленные неудачные попытки входа в систему из Гонконга, и, поскольку у вас нет там офисов или клиентов, то понимаете, что велика вероятность атаки злоумышленника. Или видите файл, содержащий вредоносное ПО, который сотрудник пытался загрузить на ваш SharePoint-сервер. Обладание данной информацией в режиме реального времени поможет избежать взлома или утечки данных.

Отслеживайте всю файловую активность в соответствии с нормами конфиденциальности

Информация о файловой активности организации в реальном времени, безусловно, является преимуществом, но только в том случае, если она охватывает каждый канал обмена данными, каждый файл. CISO Dashboard позволяет отслеживать все действия вплоть до файлового уровня, включая информацию о пользователях, временных отметках и IP-адресах. Настраиваемая CISO Dashboard подключается как к локальным, так и облачным хранилищам данных, что позволяет регистрировать каждую загрузку, скачивание и передачу файлов. Представьте, что CISO Dashboard – это история браузера вашей организации, но вместо отслеживания веб-сайтов, которые посещают ваши сотрудники, она предоставляет информацию о файлах, с которыми они работают.

Когда сотрудники информационной безопасности получат полную видимость, они будут иметь цельную картину движения каждого файла, проходящего через организацию. Надёжная CISO Dashboard позволяет отслеживать и логировать файловую активность для дальнейшего анализа или создавать детальные отчёты, которые могут продемонстрировать соответствие таким нормативным требованиям, как HIPAA, GDPR, GLBA, CCPA и другие.

Accellion

Accellion *– безопасная платформа, помогающая ИТ и ИБ-руководству контролировать обмен конфиденциальной корпоративной информацией.*

www.accellion.com | support@accellion.com

headtechnology
it-security distribution

HEADTECHNOLOGY Group *– специализированный дистрибутор, ориентированный на развивающиеся рынки Центральной и Восточной Европы, Балтии, стран СНГ и Центральной Азии.*

www.headtechnology.com | info@headtechnology.com

HEADTECHNOLOGY GROUP – глобальный партнёр вашего успеха

HEADTECHNOLOGY Group – специализированный дистрибьютор решений по информационной безопасности, ориентированный на развивающиеся рынки Центральной и Восточной Европы, Балтии, стран СНГ и Центральной Азии.

Наша компания представляет лучших в своём классе производителей решений по ИТ-безопасности, среди которых технологические лидеры, признанные гигантами аналитики Gartner, а также новаторы рынка информационных технологий.

Роль информационной безопасности в современном мире

Общеизвестно, что введение компьютеров в различные сферы деятельности человека привело к тому, что самая разнообразная информация, хранимая в электронном виде, увеличилась до объёмов, которые трудно осознать. Эти процессы были, вне всякого сомнения, оправданы, ведь в электронном виде информацию хранить проще: большие объёмы данных можно быстро копировать, переписывать, передавать на большие расстояния. Однако есть в подключении компьютера к глобальным сетям и отрицательные стороны: при отсутствии должной степени защиты ваша информация может пострадать от атак через сеть или Интернет.

Потеря коммерческой информации, её раскрытие злоумышленниками или конкурентами, скорее всего, приведёт к убыткам на рынке. Так, кража информации может понизить репутацию фирмы, а что касается её подмены, то это и вовсе может привести к разорению, не говоря уже о доверии клиентов.

Но проблемы информационной безопасности ныне волнуют не только предпринимателей. Каждый, кто хоть немного знаком с компьютером и сетью интернет знает, насколько неприятно, когда твоя информация попадает в чужие руки. И неважно, будь то письма электронной почты или информация, набираемая вами в текстовых редакторах. Потеря конфиденциальности – серьёзный психологический удар.

Интересно обратить внимание на следующую статистику, отображающую то, какие же можно назвать первоочередные причины повреждения, хищения или утраты информации:

- вследствие неумышленных ошибок, сделанных самим человеком – владельцев информации – 52%;
- вследствие умышленных действий – 10%;
- вследствие перегрева носителей и пожаров – 15%;
- вследствие повреждения водой, попавшей извне, или конденсата внутри – около 10%.

Оставшиеся проценты тем или иным образом связаны с действиями злоумышленников в сети.

Если электронная информация так подвержена хищению, подмене или уничтожению, конечно же, её следует тщательно защищать.

Headtechnology – гарант безопасности вашего бизнеса

Headtechnology представляет лучших в своём классе производителей решений по ИТ-безопасности, среди которых технологические лидеры, признанные гигантами аналитики Gartner, а также новаторы рынка информационных технологий. Портфель решений соединяет в себе традиционные потребности ИТ-безопасности и защиты от новых рисков и угроз, а также мощную защиту интеллектуальной собственности и наиболее ценных корпоративных активов клиентов.

В портфель решений Headtechnology входят вендоры, признанные GARTNER:

- Семь лет подряд MobileIron признан лидером в Магическом Квадранте Gartner в категории «ПО для управления мобильными устройствами».
- Proofpoint сохраняет бесспорное лидерство в Магическом Квадранте Gartner в категории «Защита шлюзов электронной почты».
- ForeScout является одним из лидеров в Магическом Квадранте в категории «Контроль доступа в сеть».
- OneSpan (ранее Vasco) получил признание в Магическом Квадранте Gartner в категории «Аутентификация пользователей».
- Arista – лидер Магического Квадранта в категории «Центр обработки данных».

За 13 лет работы команда Headtechnology выполнила тысячи успешных проектов для государственных и частных компаний, промышленных и финансовых групп. Нам доверяют крупнейшие системные интеграторы и технологические партнёры.

Будем рады сотрудничеству!

---

headtechnology
it-security distribution

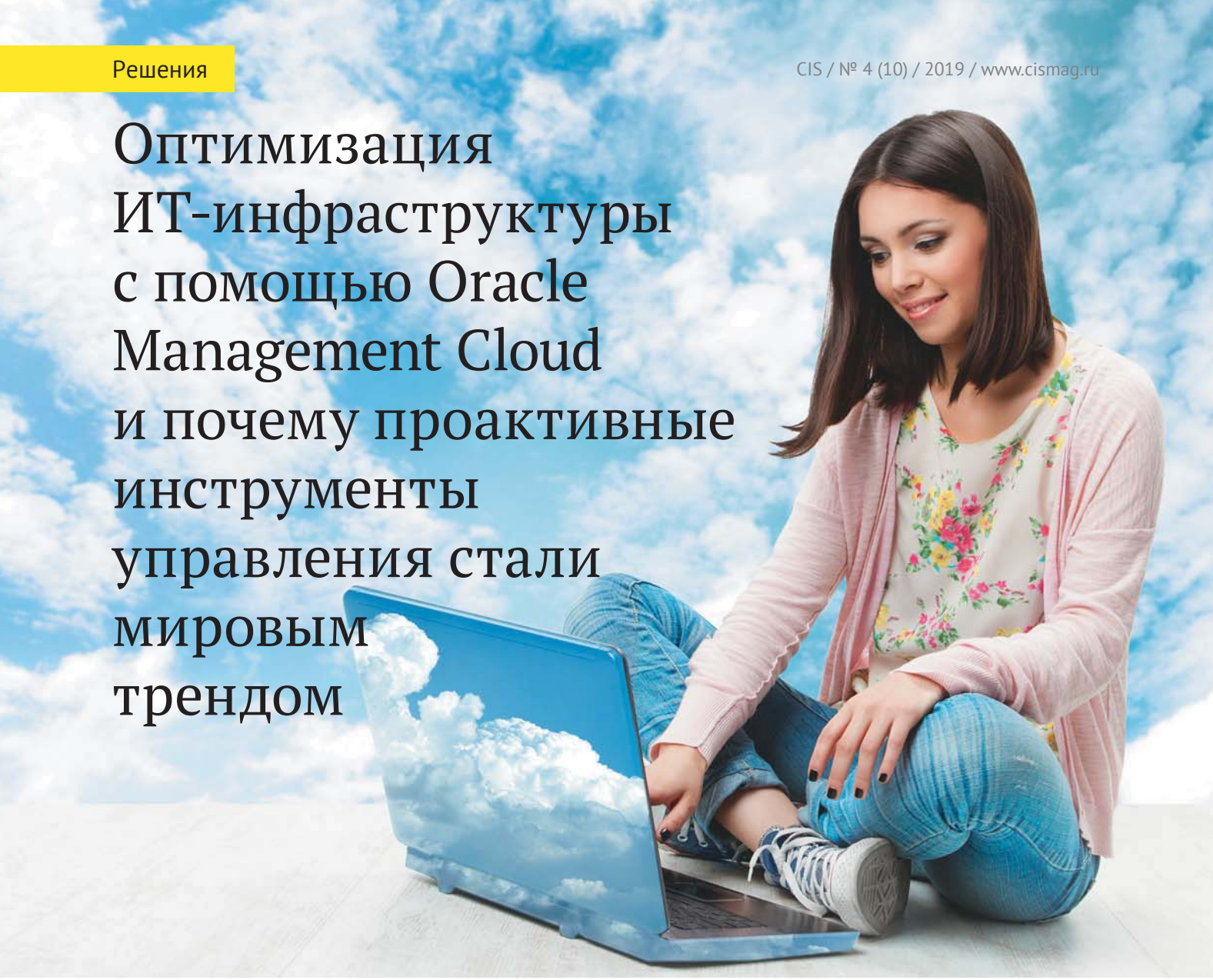
***Headtechnology Group** – надёжный дистрибьютор по комплексным решениям защиты информации вашего бизнеса.*

headtechnology.com

info@headtechnology.com

CIS / № 4 (10) / 2019 / www.cismag.ru

Оптимизация ИТ-инфраструктуры с помощью Oracle Management Cloud и почему проактивные инструменты управления стали мировым трендом



Алексей Котельницкий, руководитель группы развития облачных сервисов «ФОРС Дистрибуция»

Сегодня для ИТ любого бизнеса критическим становится вопрос скорости принятия решений, что напрямую сказывается на эффективности управления.

Зачастую задача заключается в локализации проблемы, поиске её в бизнес-приложении, состоящем из множества компонентов, баз данных, серверов приложений, которые установлены на разных физических и виртуальных серверах. Для подобных задач требуются специализированные инструменты, такие как облачные сервисы Oracle Management Cloud (OMC).

Сервисы OMC позволяют применять методы машинного обучения для выявления событий, которые могут привести систему к нестабильной работе или к более серьёзным проблемам. Любая информационная система в процессе работы генерирует огромные объёмы всевозможных логов. При этом известно, что даже сообщение об успешном завершении операции, поступившее с существенной задержкой от стандартного времени, может означать, что в системе уже что-то пошло не так. Человеку сложно улавливать такие нюансы. Только машина может обрабатывать диагностику, генерируемую машиной. Выявляя подобного рода скрытые проблемы, визуализируя их, сообщая специалисту-администратору, что требуется обратить внимание и принять решение, сервисы OMC позволяют управлять качеством работы информационных систем, предотвращая аварии.

Oracle Management Cloud

Oracle Management Cloud обеспечивает эффективный «про-активный» мониторинг, быструю локализацию проблем и возможность применения алгоритмов машинного обучения для задач операционной аналитики. Сервис избавляет от сложных процессов ручного мониторинга приложений, использования множества инструментов и зависимости от координированной работы отдельных групп ИТ-специалистов, необходимых для выявления первопричин проблем и принятия решений.

OMC также исключает использование множества фрагментированных систем мониторинга и анализа работы ИТ инфраструктуры, кото-

рое традиционно приводило к недостаточной прозрачности и снижению эффективности.

Сервис представляет собой набор интегрированных облачных средств мониторинга, управления и анализа ИТ инфраструктуры, основанный на технологиях машинного обучения и обработке больших объёмов диагностических данных. Oracle Management Cloud обеспечивает стабильность ИТ-служб, помогает предотвратить отказы приложений и упростить разработку продуктов за счёт тесной интеграции процессов разработки и эксплуатации (DevOps).

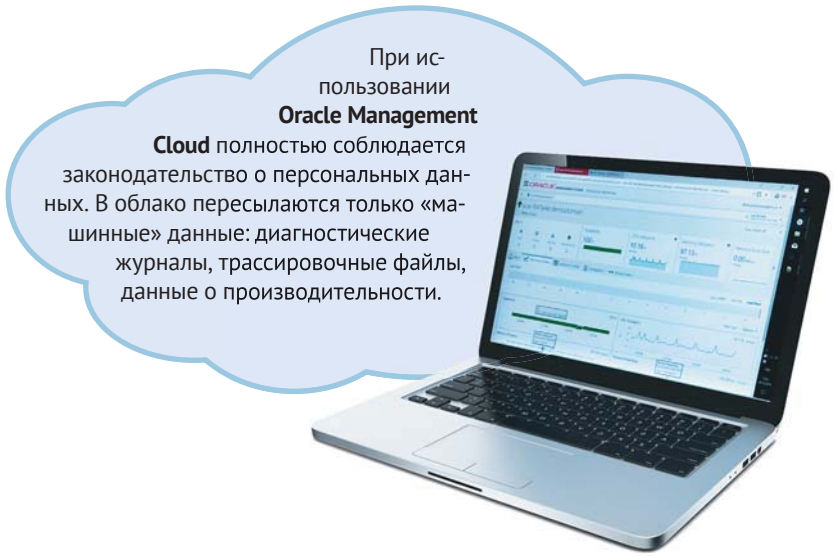
Ключевые возможности инструментов Oracle Management Cloud: мониторинг компонентов инфраструктуры, анализ пользовательского опыта, помощь в планировании мощностей и ресурсов ИТ-подразделения, анализ метрик и событий, агрегирование данных журналов событий, автоматизированное выявление аномалий и первопричин инцидентов. Исходными данными для инструментов мониторинга являются данные о работе пользователей, метрики производительности, журнальные и трассировочные файлы, данные из Oracle Enterprise Manager и других систем мониторинга, журналы аудита, диагностические данные с устройств и т.п.

Решение Oracle предназначено для применения в корпоративных центрах обработки данных (on-premise), в среде Oracle Cloud и в облачных средах других поставщиков. Основанное на горизонтально масштабируемой платформе с высокопроизводительной обработкой больших данных, это облачное решение обеспечивает глубокое понимание протекающих технологических процессов за счёт анализа работы систем в реальном времени.

Необходимо подчеркнуть важное преимущество сервисов Oracle Management Cloud: они не собирают и не передают в облако бизнес-данные или персональные данные из информационных систем! Собирается и анализируется только диагностическая информация: метрики и журнальные данные, которые при необходимости можно «замаскировать» перед отправкой в облако.

Oracle Management Cloud – гетерогенный облачный сервис для всестороннего анализа и мониторинга локальных и облачных инфраструктурных компонентов, баз данных и приложений.

Oracle Management Cloud – набор сервисов в публичном облаке, предлагаемых по подписке. Это значит, что заказчику наших партнёров нет необходимости дополнительно инвестировать и поддерживать дорогостоящую, сложную инфраструктуру для инструментов мониторинга. Всё, что требуется: установить агентов и настроить передачу данных в облако.



Основные преимущества

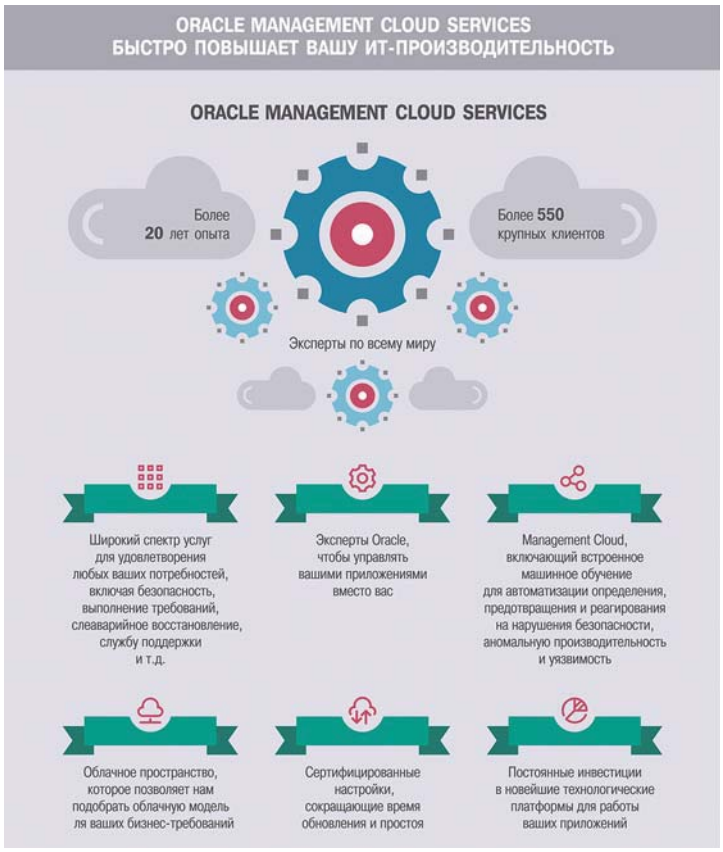
- Всесторонний мониторинг. Решение отслеживает метрики на всех уровнях: от поведения пользователей до аппаратного обеспечения серверов, системных процессов и средств резервного копирования. Как в ЦОДе, так и в облаке.
- Производительность. Отражает производительность работы приложений в реальном времени. Позволяет в онлайн режиме анализировать работу даже высоконагруженных систем.
- Безопасность. Данные передаются по шифрованному каналу, встроенные средства автоматизированного маскирования конфиденциальных данных обезличивают информацию перед отправкой в облако.
- Понятная и доступная информация. Сервис предоставляет расширенную информацию для принятия решений по устранению проблем и выявлению «узких мест» в рамках корпоративной информационной системы в целом. Наглядная графика и визуализация данных помогают быстро находить отклонения.
- Упрощение мониторинга и оптимизация ИТ. Необходимо только установить программных агентов на серверы, и диагностическая информация будет автоматически накапливаться и пересылаться в облако, после чего хранение, обработка и анализ данных происходит в ЦОДе Oracle. Подобный вариант использования не предполагает капитальных затрат.

Компоненты решения

Портфолио Oracle Management Cloud входит в состав платформенных сервисов Platform-as-a-Service (PaaS) и включает несколько сервисов:

Oracle Application Performance Monitoring Cloud Service. Мониторинг производительности web-приложений

Сервис Application Performance Monitoring позволяет диагностировать производительность приложений вплоть до уровня кода и отдельных запросов. APM позволяет службам разработки и эксплуатации (DevOps) работать в едином интерфейсе, дополняя друг друга. Мониторинг



производительности приложений осуществляется в онлайн режиме и, в случае возникновения проблем или отклонений, система отправляет оповещения ответственным специалистам. С помощью АРМ администраторы приложений могут осуществлять анализ производительности серверов приложений, скорости загрузки страниц и выполнения AJAX запросов. Предусмотрена навигация по уровням технологического стека и возможность детализировать информацию до уровня конкретной записи в журнальных файлах приложения, что позволяет легко обнаруживать и устранять «узкие места».

Oracle Log Analytics Cloud Service. Анализ журналов приложений

Сервис Log Analytics позволяет осуществлять мониторинг, агрегирование, индексирование, анализ, поиск и установление корреляции данных в журналах событий приложений и компонентов инфраструктуры (локальных и облачных) в реальном времени. Система распознаёт и группирует записи в журналах, автоматически выявляет аномальные записи и позволяет видеть только те записи, которые отражают отклонения в работе систем и приложений. Встроенная система визуализации журнальной информации позволяет создавать информационные панели, которые наглядно отображают ключевые события в системах.

Oracle IT Analytics Cloud Service. Планирование и мониторинг ресурсов ИТ-ландшафта

Инструментарий IT Analytics позволяет определять закономерности функционирования текущего ИТ-ландшафта, выявлять проблемные участки и эффективно планировать мощности. Его главные задачи:

- анализ ресурсов (выявление неравномерной нагрузки, анализ потребления ресурсов в разных разрезах и по различным периодам)
- планирование роста нагрузки на ИТ инфраструктуру
- анализ производительности ИТ инфраструктуры с использованием встроенных средств анализа диагностической информации
- выявление ресурсоемких SQL-запросов
- визуализация общей картины производительности и построение информационных панелей.

Oracle Infrastructure Monitoring Cloud Service. Система проактивного мониторинга состояния гетерогенной инфраструктуры: как локальной, так и облачной.

Упреждающий мониторинг по всем уровням позволяет администраторам заблаговременно узнавать о потенциальных проблемах, диагностировать и устранять их прежде, чем они окажут влияние на конечных пользователей. Infrastructure Monitoring позволяет выявлять аномальные значения метрик, организовать систему раннего предупреждения о проблемах, коррелировать значения метрик производительности.

Бесплатные консультации

Мы готовы проконсультировать наших партнёров и их заказчиков по всем вопросам использования сервиса. Укажите ФИО и адрес электронной почты, и мы свяжемся в течение рабочего дня.

Бесплатный POC/POV

POC (Proof-of-Concept) или POV (proof-of-value), подтверждение концепции – это возможность оценить применимость продуктов и сервисов на реальных задачах. Это полноценный пилотный проект с достоверными результатами для обоснования выбора и принятия решения.

Расширенная техподдержка ИТ-инфраструктуры

Команда «ФОРС Дистрибуции» осуществляет круглосуточный мониторинг и диагностику информационных систем, разрабатывает рекомендации по оптимизации инфраструктуры с учётом меняющейся нагрузки.

Настройка и развёртывание сервисов OMC

Поможем использовать максимум возможностей OMC нашим партнёрам, осуществим настройку мониторинга объектов ИТ-инфраструктуры, включая нестандартные объекты, с учётом нашего опыта порекомендуем настройку и использование информационных панелей для полноценного мониторинга инфраструктуры.

Обучение

Наши эксперты проводят авторские курсы для партнёров и их заказчиков на основе уникальных материалов, а также очные и дистанционные тренинги для специалистов с разным уровнем подготовки. Предоставляем облачные среды для самостоятельной подготовки.

Сайт Oracle

Вы можете узнать больше об Oracle Management Cloud Service в соответствующем разделе на сайте Oracle.com и в блоге Oracle в России https://blogs.oracle.com/russia/.

Опыт «ФОРС Дистрибуции»

За последние годы «ФОРС Дистрибуция» накопила обширный опыт использования сервисов Oracle Management Cloud в собственном частном облаке, а также в ряде проектов с партнёрами и заказчиками. Кроме того, «ФОРС Дистрибуция» регулярно проводит тренинг по работе с сервисами Oracle Management Cloud для партнёров и заказчиков.

По запросу Oracle, в рамках международного обмена опытом, специалисты компании также провели данный тренинг для партнёрских обучающих центров в ряде стран: Россия, Польша, ЮАР, Кения, Турция, Италия, Англия, Швейцария, Саудовская Аравия, Нидерланды. Обучение позволило ИТ-руководителям, разработчикам, администраторам и архитекторам получить практические знания по эффективному использованию облачных технологий, возможностям повышения стабильности ИТ-инфраструктуры, ускорению работы приложений, оперативному выявлению, рассмотрению и решению возникающих проблем.

«ФОРС Дистрибуция» постоянно совершенствует механизмы взаимодействия с партнёрами, стараясь сделать решение повседневных бизнес-задач каждой компании максимально эффективным.

В 2018 г. «ФОРС Дистрибуция» получила награду за выдающийся вклад в развитие Oracle Management Cloud на Oracle EMEA PaaS Partner Community Forum 2018.
Развитие облачных сервисов Oracle – одно из приоритетных направлений «ФОРС Дистрибуции».

ФОРС ДИСТРИБУЦИЯ

«ФОРС Дистрибуция» *– платиновый партнёр и дистрибутор корпорации Oracle в России и Монголии, активно развивает направление, связанное с облачными технологиями Oracle. Компания была основана в 2011 г. на базе центра по работе с партнёрами компании «ФОРС – Центр разработки», признанного на российском рынке эксперта в области технологий Oracle. Основными составляющими бизнеса «ФОРС Дистрибуция» на сегодняшний день являются: дистрибуция ПО, облачных сервисов и аппаратных систем Oracle, технологический консалтинг и обучение технологиям Oracle, оказание услуг по тестированию и миграции комплексных решений в рамках многофункциональной инновационной площадки FORS Solution Center. Персонал компании имеет более чем 20-летний опыт работы с продуктами Oracle. Продажи продуктов и решений Oracle осуществляются исключительно через партнёрскую сеть, ключевая роль в формировании и поддержке которой принадлежит дистрибутору.*

www.partner.fors.ru

SafeNet ProtectV – безопасность виртуальных машин

«Магия» виртуализации & облаков

Плотность виртуализации ⟷ Переход в облака

- 40% серверов виртуальные
- Средняя* организация: 470 VM, 200 критичны для бизнеса
- К 2020 85% нагрузки на виртуальных серверах

* США, Европа

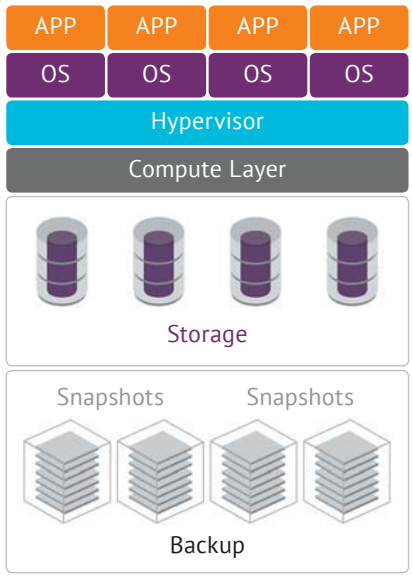
60% организаций с «виртуализацией» думают → тестируют → переходят → в частное/публичное облако

Облака упрощают работу с данными

Перемещение данных в облако – это не просто...

- Кто владеет нашими ключами шифрования в облаке?
- А соответствуем ли мы требованиям регуляторов?
- А сможем ли мы защитить конфиденциальные данные?
- Как мы контролируем интерес «госорганов», при проверках сервис-провайдера?
- Как мы предотвратим доступ к нашим данным администраторов и «соседей» по облаку?
- Как нам быть уверенными, что мы, действительно, удалили все данные?
- Как централизовать управление безопасностью в нескольких облачных средах?

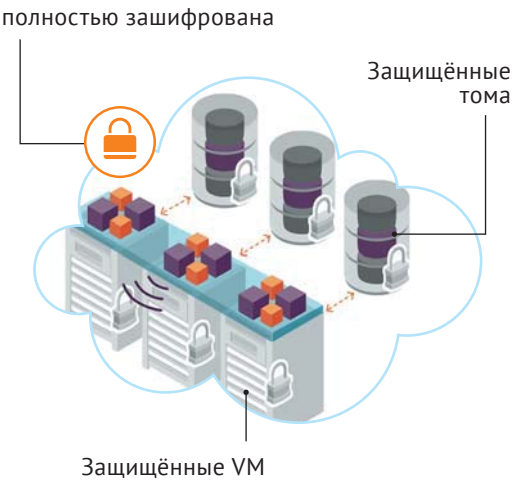
Очень легко потерять контроль



- VM легко скопировать и украсть
- VM легко перенести на другой сервер
- Появился новый класс привилегированных пользователей (администраторы серверов, хранилищ, архивов)
- Может быть много копий VM, «снапшотов», архивов
- Проблема удаления данных VM при необходимости

ProtectV – обеспечивает полное шифрование VM

- **Шифрование всей VM**
  - Разделы с ОС
  - Разделы с данными
- **Шифрование всех связанных «снапшотов» и резервных копий (DR-сайты, и т. п.)**



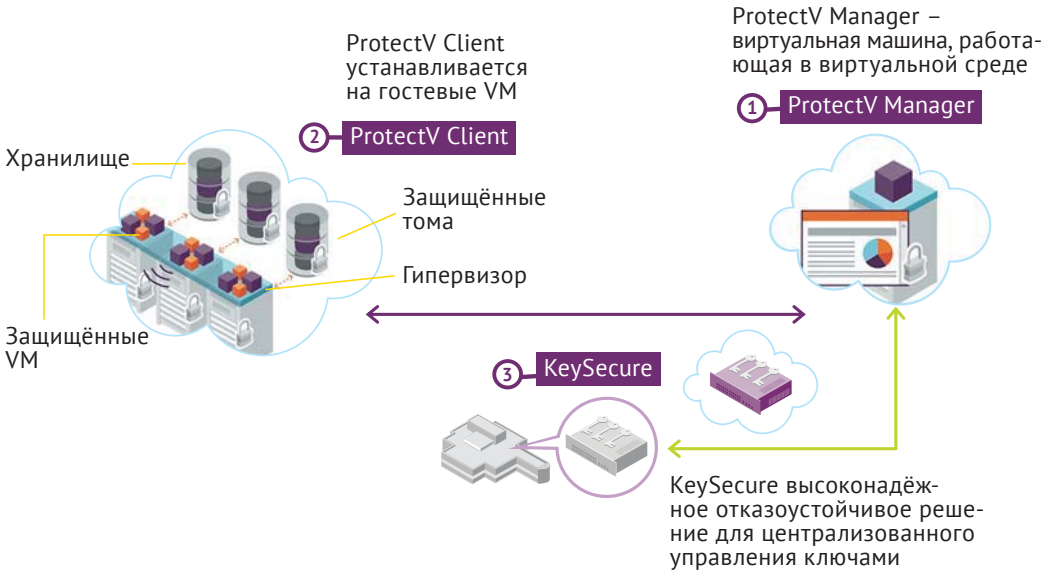
Защита данных для виртуальной среды

ProtectV – промышленное решение по защите данных для виртуальной и облачной инфраструктуры.
Решение обеспечивает:

- **изоляцию** данных
- **авторизованный запуск** VM
- **контроль доступа** ко всем копиям VM и дисков
- полную **блокировку** доступа в случае компрометации

ProtectV – возможность **безопасно** переносить важные элементы ИТ-инфраструктуры в «не доверенную» или общедоступную среду.

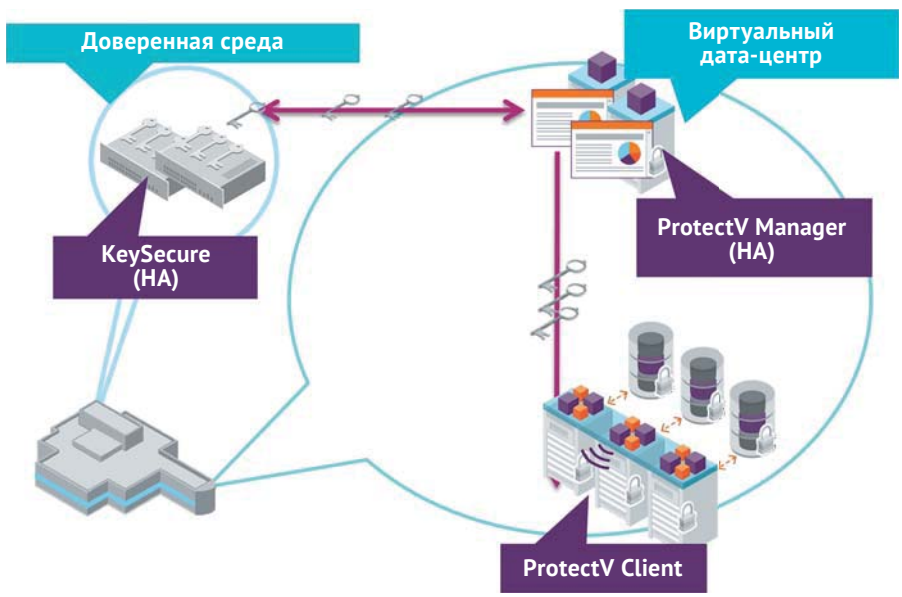
Анатомия защиты данных в виртуальной среде



KeySecure

- Сервер формата 1U с опциональным HSM внутри
- Аппаратный RAID и два блока питания
- 4 настраиваемых Ethernet-порта для сегментации
- Есть виртуальные апплаенсы для разных платформ виртуализации

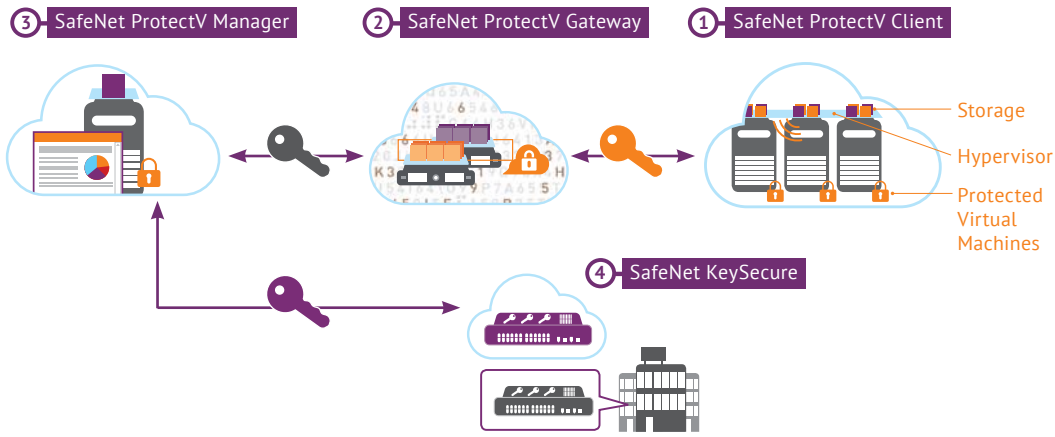
Пример: виртуальный дата-центр



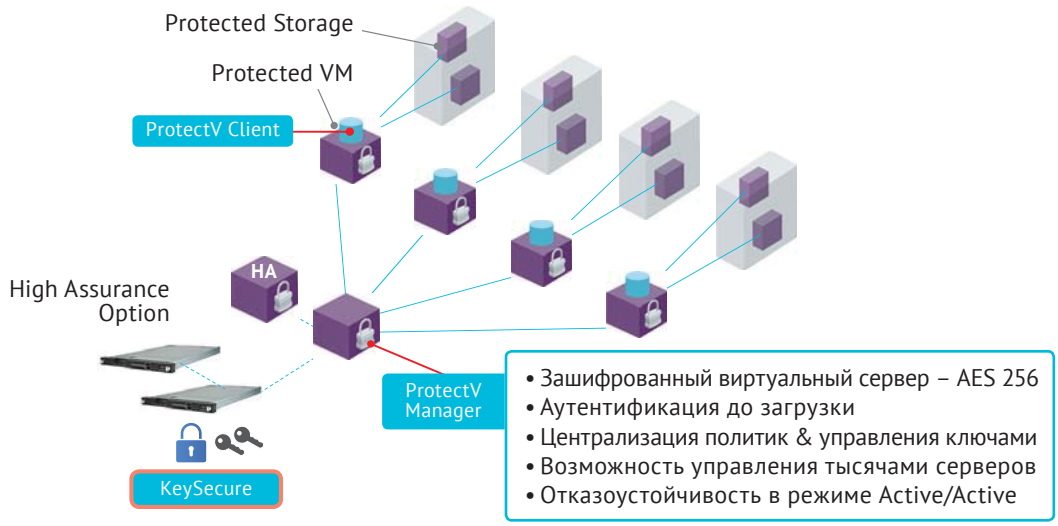
Инфраструктура VMware

Защищаем ресурсы на разных виртуальных площадках

PV-шлюз размещается отдельно от PVM, на виртуальной площадке вместе с защищаемыми виртуальными серверами.



ProtectV – возможности масштабирования



ProtectV: поддерживаемые среды, продукты, производительность

- ProtectV сейчас поддерживает:
  - VMware vSphere
  - Microsoft HyperV
  - Amazon Web Services EC2
  - Amazon Web Services VPC
  - Microsoft Azure
  - IBM Bluemix
  - Google Cloud Platform
- ProtectV – влияние на производительность 5% – 10%
- Совместимые системы управления ключами шифрования:
  - SafeNet KeySecure (k250, k460, k450)
  - SafeNet Virtual KeySecure (k150v, k170v)

Поддерживаемые операционные системы

Microsoft Windows (64-bit)
- 2008R2/2012/2012R2/2016; Window 7, 10

Red Hat Enterprise Linux
- 6.5-7.5 (64-bit)

Linux CentOS
- 6.7,6.8,6.9,7.3,7.4 (64-bit)

Linux SUSE Server
- 11SP4/12SP264-bit

Ubuntu, Oracle, Amazon Linux

Основные сценарии использования

Для предприятий
- Контроль данных в виртуальной среде
- Изоляция данных на «общих» СХД
- Перенос инфраструктуры во внешний дата-центр (к сервис-провайдеру)
- Резервная площадка в облаке
- Неизвлекаемость данных при краже, захвате СХД
- Разграничение полномочий между привилегированными пользователями
- (администраторами СХД, виртуальной инфраструктуры и ИБ)
- Соответствие требованиям «регуляторов» (PCI DSS)

ProtectV – лицензирование

По числу виртуальных серверов, на которые будет производиться инсталляция агента ProtectV.

Аппаратный или виртуальный SafeNet KeySecure Возможна кластеризация для отказоустойчивости.

Пример спецификации:

Product	Price	Q-ty	Total
ProtectV Client, CAPEX	$1300	10	$13000
Virtual KeySecure, CAPEX	$12000	1	$12000
One Year of Standard Maintenance Service	18%		$4500
Total	Total		**$29500**

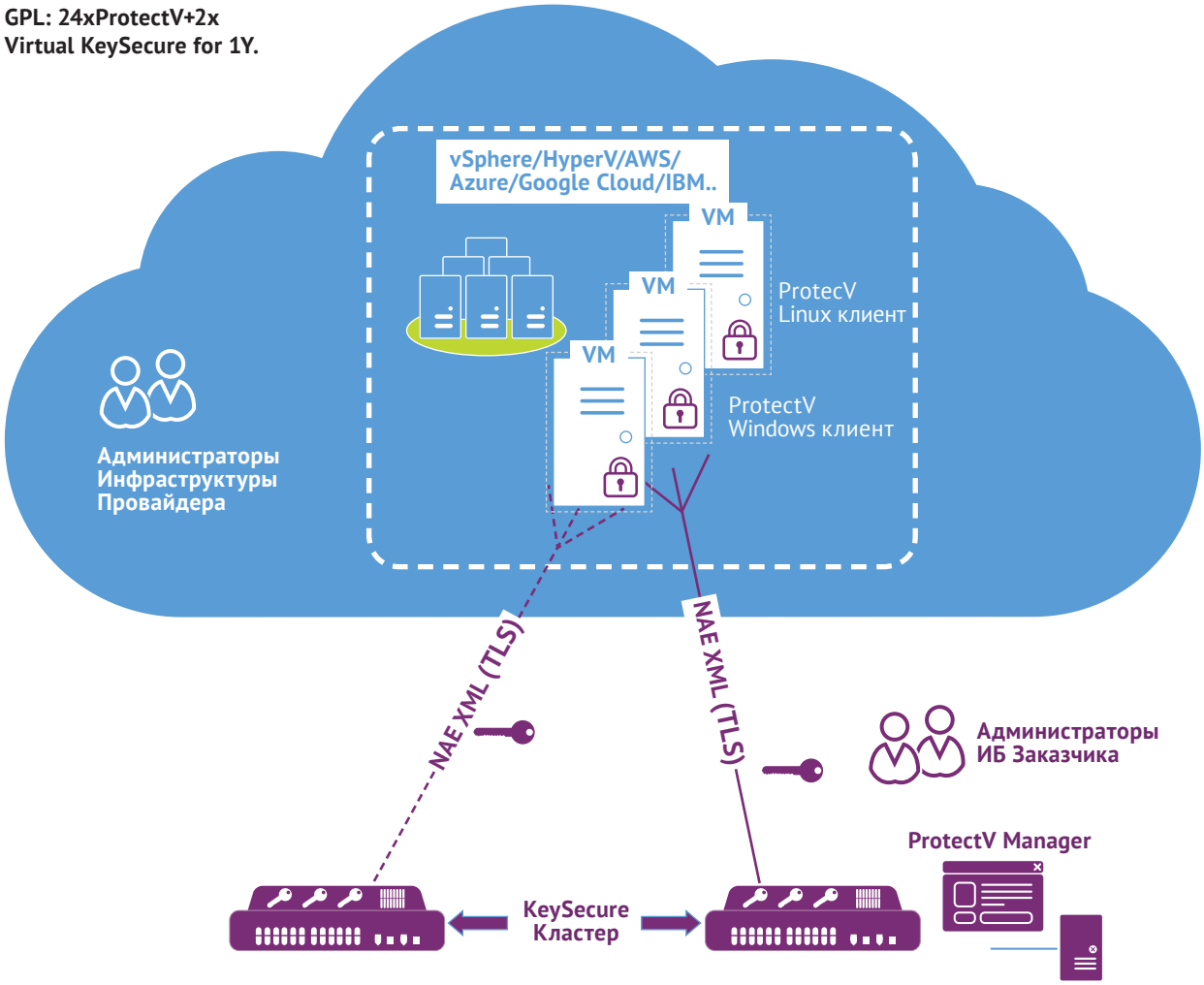
Возможен OPEX – 1-3 года

Защита данных на разных уровнях «стека Рисков»

Уровни защиты	Учтённые риски		
Приложения/БД	Уровень App/DB DBAdmins, DB Users		SafeNet/Vormetric ProtectApp
Файловая система	**Контроль на уровне ОС** User/groups for System/ LDAP/AD/ Hadoop/Containers Includes Privileged/ Root Users for APT/Malware protection		SafeNet/Vormetric Transparent Encryption
Диск	**Кража /утеря физич. и виртуальных носителей**		KMIP Key Management & SAFENET PROTECTV

Защита виртуальных машин в облаке партнёра (IaaS)

GPL: 24xProtectV+2x Virtual KeySecure for 1Y.



Заказчик: Финансовая организация. Партнёр: Российский IaaS провайдер.

Объект: 24 виртуальных сервера CENTOS, размещённых в облаке сервис-провайдера.

Решение: Для решения задач раздельного управления средой виртуализации и защиты виртуальных машин (разделение полномочий) было выбрано шифрование виртуальных машин VMware средствами ProtectV с размещением ключей в защищённом хранилище KeySecure (кластер виртуальных апплаенсов), расположенном вне виртуальной среды провайдера. Также рассматривалось и тестировалось нативное шифрование VMware (VMCrypt) с использованием внешнего ключевого хранилища KeySecure, но по ряду требований безопасности Заказчик и Провайдер отказались от него в пользу ProtectV. Выбранный подход и решение имеют ряд преимуществ по сравнению с нативным шифрованием VMWare:

1. Управление шифрованием в ProtectV осуществляется отдельно от среды виртуализации в среде ProtectV Manager. В VMCrypt – это администраторы vCenter.
2. В ProtectV для запуска виртуальной машины требуется доступ к ключевому хранилищу KeySecure. В VMCrypt ключи шифрования находятся в памяти Гипервизора, и VM можно перезапускать, пока работает ESXi при отсутствии доступа к KeySecure.
3. В ProtectV есть защита от клонирования VM. VM при запуске проходит процедуру аутентификации, и если запуск клонов не разрешён, она не может быть запущена без разрешения администратора ИБ. В VMCrypt зашифрованные копии или снапшоты могут быть подключены к любой VM и запущены без предварительной аутентификации.
4. ProtectV предлагает централизованный механизм управления шифрованием виртуальных машин в различных виртуальных и облачных средах. VMCrypt – только отдельная среда VMware.

PRODUCT BRIEF
SafeNet ProtectV™

Гарантированная безопасность и соответствие требованию регулятора внутри облачной и виртуальной инфраструктуры

Решение SafeNet ProtectV предоставляет функционал шифрования всех дисковых разделов физических, виртуальных машин и облачных экземпляров таким образом, что вы можете осуществлять хранение и обработку критической информации даже при условии её размещения вне контролируемого периметра. SafeNet ProtectV гарантирует защиту данных при их размещении и обработке в облачных средах Amazon Web Services, Microsoft Azure, IBM Bluemix, а также средах виртуализации VMware и Microsoft Hyper-V.

Первое комплексное индустриальное решение с высокой доступностью для защиты физической, виртуальной и облачной инфраструктуры SafeNet ProtectV позволяет полностью шифровать сервера и смонтированные разделы с данными, защищая последние от несанкционированного доступа. В дополнение к сказанному, компоненты решения ProtectV Manager и ProtectV Client не могут быть запущены без прохождения процедуры аутентификации и авторизации в модуле доверенной загрузки SafeNet ProtectV StartGuard.

С помощью механизмов шифрования, реализованных в SafeNet ProtectV, организация всегда будет уверена, что доступ к зашифрованным данным и ключам шифрования доступны только ей.

SafeNet ProtectV позволяет вам защищать данные в облачных и виртуальных средах

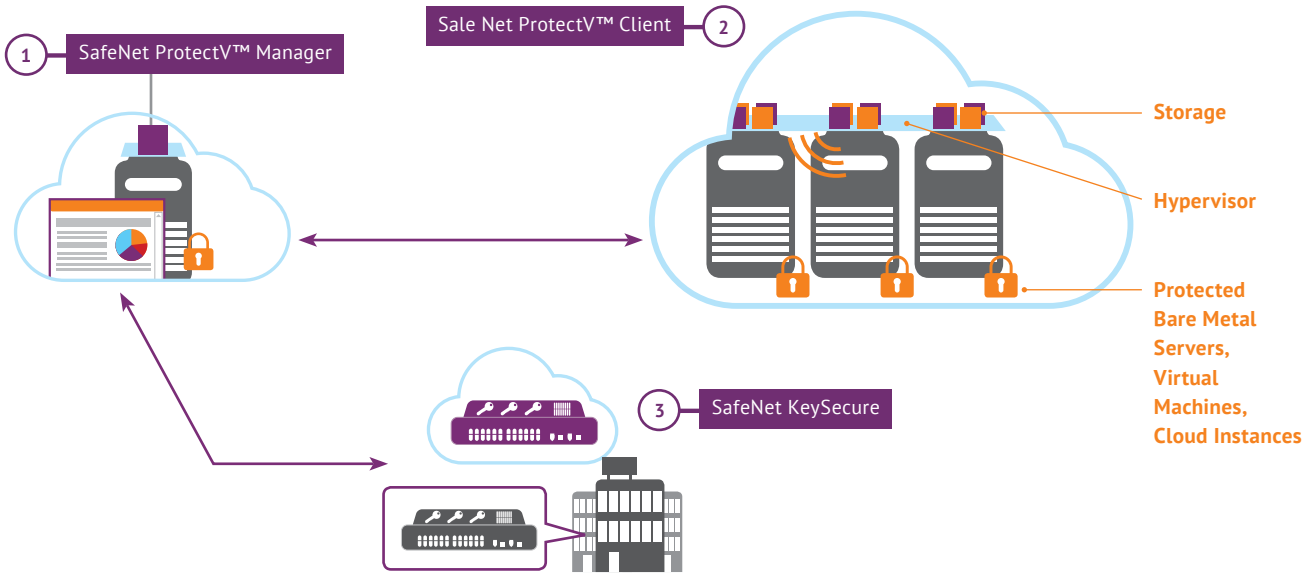
- Изоляция серверов и хранилищ через шифрование системных разделов и разделов с данными
- Доверенная загрузка с помощью SafeNet ProtecV StartGuard для авторизованных пользователей
- Контроль доступа к ключам, используемых для защиты всех копий данных
- Отзыв ключа шифрования после завершения работы с данными

Совместно с решением SafeNet KeySecure SafeNet ProtectV предоставляет высоко доступное решение по шифрованию, отвечающее требованиям индустриальных стандартов по безопасности, таких как PCI DSS, GDPR, HIPPA HITECH. Дополнительно решение позволяет чётко разделить обязанности администратора по безопасности с возможностью предоставления отчётов о соответствии требованиям регулятора.

1. SafeNet ProtectV Manager – централизованная консоль управления для шифрования физических, виртуальных и облачных машин.

2. SafeNet ProtectV Client – агент, инсталлируемый на физическую, виртуальную или облачную машину, обеспечивающий процедуру доверенной загрузки, шифрования и распределения политик безопасности со стороны SafeNet ProtectV Manager.

3. SafeNet KeySecure – решение для управления жизненным циклом ключей. Поставляется в виде аппаратного или виртуального устройства.



Техническая спецификация

Поддерживаемые облачные и виртуальные платформы:

- Amazon: Amazon EC2, Amazon VPC, Amazon GovCloud
- VMware vSphere
- Microsoft: Azure, Hyper-V
- IBM Bluemix: IBM Bare Metal и Bluemix VMs

Минимальные системные требования:
SafeNet ProtectV Manager:

- AWS: m^3. medium и выше
- IBM Bluemix: минимум Private 1 x 2.0 GHz Core
- Microsoft Azure: минимум Standard A2
- Microsoft Hyper-V: Ubuntu [Linux 64-bit], 2vCPU, 4GB памяти (минимум), 1 NIC [VMXNET 3], 16Gb дискового пространства
- VMware vSphere: Ubuntu [Linux 64-bit], 2vCPU, 4GB памяти (минимум), 1 NIC [VMXNET 3], 16Gb дискового пространства

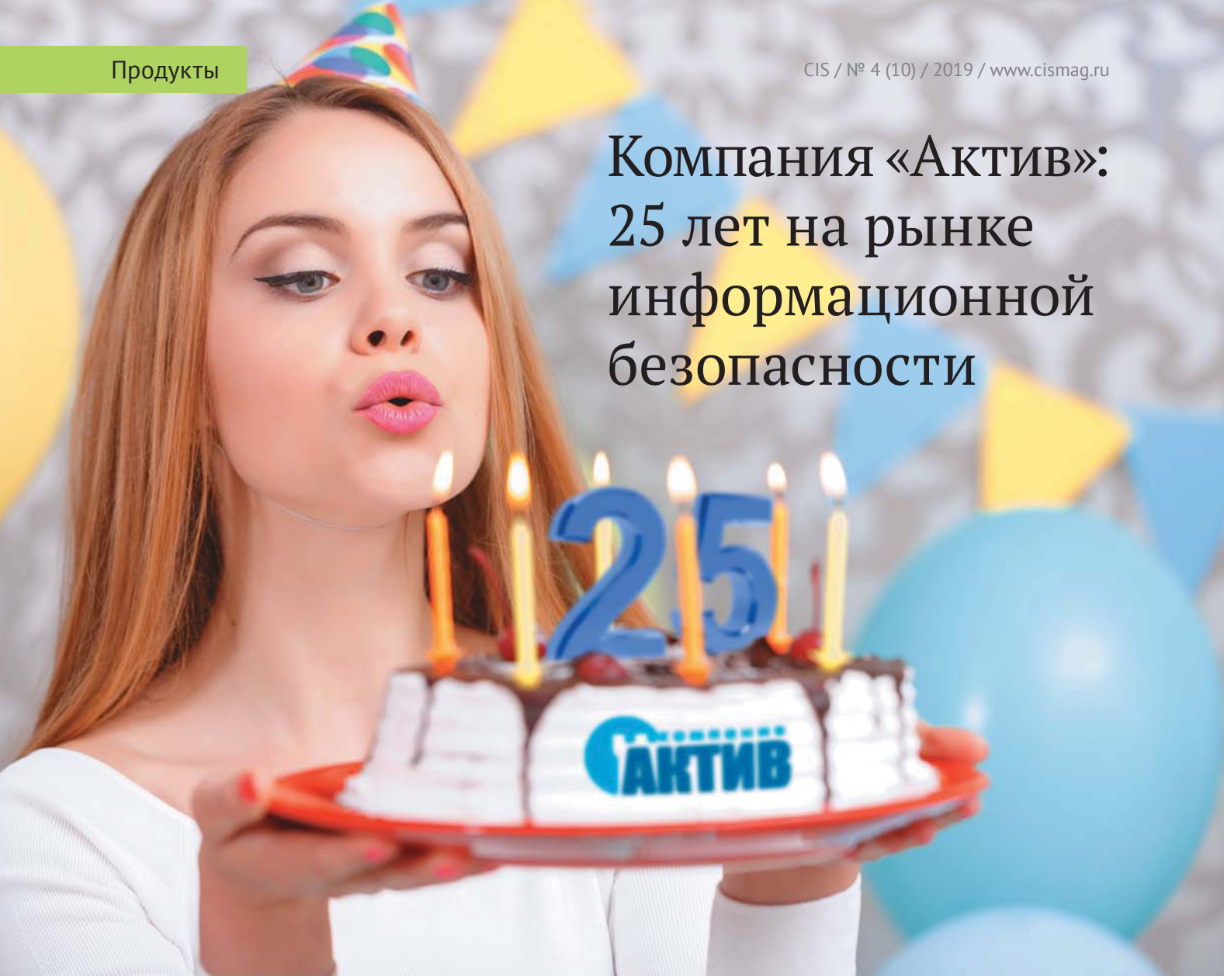
SafeNet ProtectV Client:

- Windows: 256 MB RAM, 100MB свободного дискового пространства
- Linux: 256 MB RAM, 100MB свободного дискового пространства
- AWS (только): экземпляр должен быть больше, чем micro (t1. micro не поддерживается)

Гостевые операционные системы:

- Microsoft Windows Server
- Microsoft Windows 7
- Amazon Linux
- CentOS
- Oracle Linux
- Red Hat Enterprise Linux (RHEL)
- SUSE Linux Enterprise Server (SLES)
- Ubuntu

Компания «Актив»: 25 лет на рынке информационной безопасности



Наверное, не найдётся на рынке информационной безопасности человека, который бы не знал, или хотя бы не слышал об одном из его ветеранов – компании «Актив». Даже если вы никогда не слышали название этой компании, то почти наверняка торговые марки Guardant и Рутокен окажутся знакомыми.

История компании началась в конце 1980-х годов, когда её основатели, будучи студентами, занимались научно-техническим творчеством молодёжи, как это называлось в те времена. Официально же компания была зарегистрирована ровно 25 лет назад.

Доверие

С чего начинается бизнес в сфере информационной безопасности? Вопрос не праздный, но наши собеседники сошлись в одном – с доверия. Без доверия поставщику, разработчику, интегратору невозможно успешно реализовать ни один проект, связанный с безопасностью. Тогда, в середине 90-х годов, основателям компании удалось завоевать доверие заказчиков и поставить первые партии ключей для защиты программного обеспечения, которые сейчас известны под маркой Guardant. Потом на рынок выводились другие продукты, но первые уроки основатели выучили накрепко.

Уроки состояли в том, что на рынке безопасности продукт должен просуществовать довольно долго, чтобы заказчики смогли ему доверять. Поэтому все проекты по разработке ведутся с расчётом на то, что продуктовый цикл будет довольно длительным и отдача от вложений придёт далеко не сразу.

Игра вдолгую, работа на перспективу влияет на всю деятельность компании и на людей, в ней работающих.

Люди

Люди, специалисты – это главное богатство ИТ-компании и, наверное, одна из главных составляющих долговременного успеха. Сотрудники, чьими силами разрабатываются, производятся и поддерживаются продукты, приносящие доход, настроены на долгосрочное сотрудничество с компанией. Несмотря на то, что коллектив достаточно молодой, есть и довольно много «ветеранов», чей стаж в компании более 10 лет. По нынешним временам это очень большой срок, но именно так обеспечивается глубокое погружение в решение долгосрочных задач. Сотрудники понимают и разделяют эту стратегию,

и поэтому в компании практически нет текучки кадров.

В «Активе» созданы все условия и возможности для профессионального роста и раскрытия творческого потенциала. Подтверждение этому – высочайший уровень компетенции и экспертизы по ключевым направлениям Рутокен и Guardant. Многое делается для того, чтобы в коллективе была атмосфера доброжелательности и сотрудничества.

Интеллектуальный багаж компании развивают и приумножают более 160 высококвалифицированных специалистов.

Кузница кадров

В то время как множество работодателей страдают от нехватки квалифицированных кадров, особенно молодых, «Актив» не сидит сложа руки и не ждёт милостей от «Минобра». Компания воспитывает собственный кадровый резерв, активно взаимодействуя с образовательными учреждениями. Ежегодно здесь проходят практику десятки студентов, которые практически сразу погружаются в решение не абстрактных, а вполне конкретных задач. Практически каждый получает задание по душе и по способностям, поскольку «Актив» – это многопрофильная компания, работающая на самых разных уровнях. Здесь и проектирование электронных устройств, и разработка микропрограмм, прикладного софта, веб-приложений и масса всего другого.

Многие из тех, кто проходил практику, будучи студентами, уже по несколько лет работают в компании, имея все возможности для карьеры и развития.

Партнёрство

Не имей сто рублей, а имей сто друзей – этим принципом компания руководствуется с самого начала. Партнёры не только помогают продавать, но и активно участвуют в развитии компании. В своё время было принято решение всеми силами добиваться поддержки электронных идентификаторов Рутокен в самых разных продуктах из области информационной безопасности, государственных и корпоративных информационных системах, всевозможных операционных системах и на разных платформах. Это не могло не дать результата, и на сегодняшний день, наверное, не найдётся другого столь же универсального продукта.

Многие продукты родились благодаря партнёрству. Самый известный из них – Рутокен Lite, который сперва был сделан как заказной ключевой носитель для удостоверяющего центра СКБ «Контур», а впоследствии стал одним из самых популярных носителей на рынке, по сути, стандартом де-факто.

Другим примером успешного сотрудничества в разработке новых продуктов при участии заказчиков является устройство для криптографической защиты информации при межмашинном взаимодействии и в интернете вещей.

Компания продолжает расширять партнёрское сотрудничество, наращивая не только количество партнёров, но и их качество, делясь компетенциями и опытом. В 2018 году партнёрская сеть выросла более чем на 75 новых организаций. В основном это российские компании, которые могут предложить эффективные и конкурентные решения. Были подписаны соглашения с новыми разработчиками, системными интеграторами и крупными дистрибьюторами. Ведётся ряд проектов для крупных заказчиков. Доля последних увеличилась за прошедший год на 10%, в основном за счёт сотрудничества с госкорпорациями.

Импортозамещение

Сейчас только ленивые не говорят об импортозамещении, цифровом суверенитете и тому подобных вещах. С момента основания стратегия компании основывалась на разработке собственных решений и производстве продуктов на территории РФ. По словам сотрудников, компания занималась импортозамещением, когда и слова такого ещё не было – просто делали собственные продукты, не задумываясь о том, как это назовут.

Все ключевые технологии держались и держатся под собственным контролем: от разработки схемотехники и микрокода до автоматизации производства.

Возможно ли называть импортозамещением производство, в котором используются иностран-

1996 – Guardant Stealth LPT
В прошлом веке компания была известна как производитель электронных ключей, которые подключались к LPT-порту. Эти устройства были прозрачны для принтеров, поэтому в названии есть слово Stealth.

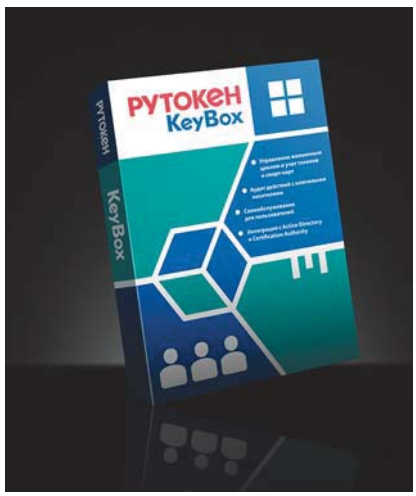
2001 – Guardant Stealth II
Первые электронные ключи Guardant для USB-порта, отдалённо похожие на современные Рутокены, компания начала предлагать своим клиентам на рубеже веков.

2007 – СКЗИ Рутокен
СКЗИ Рутокен. Сертификат ФСБ России получен в далёком 2007 году. Это первый сертифицированный криптографический токен в России.

2013 – Рутокен ЭЦП micro
В 2013 году компания начала производить электронные идентификаторы в микро-исполнении. Вычисляют электронную подпись «на борту», как и классические токены.

2013 – Рутокен ЭЦП 2.0
Универсальный токен, флагман линейки Рутокен. Появился на свет в счастливом для компании 2013 году.

2013 – Рутокен ЭЦП Bluetooth
В том же году появился Рутокен ЭЦП Bluetooth. Первое и единственное устройство, позволяющее работать с электронной подписью на мобильных устройствах через Bluetooth.



2013 – Рутокен KeyBox
В том же году появилось ПО Рутокен, которое можно было купить за деньги. До этого весь софт Рутокен был только бесплатным.

ные комплектующие? Специалисты «Актива» считают, что возможно, хотя и не без оговорок. Пока отечественная электронная промышленность не в состоянии обеспечить всех потребностей, но компания стремится как можно больше локализовать производство, а вся разработка происходит в России. Об этом свидетельствует наличие продуктов «Актива» в едином реестре отечественного ПО.

Импортозамещение – это ещё не всё, чем может похвастаться «Актив». Ряд продуктов успешно экспортируется не только в страны бывшего СССР, но и в Европу, и даже в Юго-Восточную Азию.

Производство

Каково это – быть российским производителем электроники? Заниматься производством чего бы то ни было – это вообще непростая задача, а тем более – сложной высокотехнологичной продукции в наших непростых условиях.

Компания «Актив» имеет своё собственное производство. Развитие технологического процесса шло по пути автоматизации сборки и контроля качества. Постоянная работа по улучшению качества привела к тому, что многие средства производства спроектированы или произведены сотрудниками компании: средства входного контроля электронных модулей (составная часть изделий), устройства для программирования и контроля качества.

Производство состоит из опытной экспериментальной площадки для разработки инновационных продуктов, оборудования для проверки электронной части изделий, программирования и маркировки, оборудования для производства пластиковых корпусов, сборочного участка, участка контроля и инструментального цеха.

Особенность производства такова, что его мощности могут быть существенно расширены за короткие сроки. В производстве задействованы специализированные автоматические линии, которые компания проектирует и собирает собственными силами. Внедрение автоматизации не только делает производство экономически выгодным, но и выступает инновационным инструментом, повышающим конкурентоспособность компании и всей отрасли в целом.

Огромное внимание уделяется качеству. Производство электронных изделий на массовый рынок имеет много особенностей. Например, невозможно исправить программные ошибки в микрокоде и ошибки, допущенные на этапе проектирования и производства электроники, как это возможно при производстве программных продуктов. Поэтому строгое следование стандартам разработки, производства и требованиям безопасности – это базовые принципы, которым подчиняется всё в производстве программного обеспечения и электроники.

В настоящее время «Актив» производит изделия в режиме полного цикла сборки. Компания в состоянии оперативно перейти на полную российскую комплектацию изделий в случае изменения политической конъюнктуры. В настоящее время такой ход тщательно проработан. По сегодняшним ценам это привело бы к увеличению себестоимости изделий на 10-15%, что в компании считают недостаточно целесообразным. В 2018 году компания завершила комплектацию своих изделий чипами от недорогих неспециализированных западного производства до российских высокозащищённых.

Поставщики выбираются по тем же принципам, что компания исповедует в отношениях со своими партнёрами: открытость, надёжность, расположенность к сотрудничеству.

В 2018 году компания запустила собственную линию производства полного цикла по выпуску смарт-карт. Производство также находится в Москве. Смарт-карты могут быть оснащены любыми бесконтактными RFID-метками. Широкие возможности графической персонализации позволяют нанести на карту любые индивидуальные данные.

В настоящее время «Актив» обладает современным производственным комплексом. Ключевая компетенция компании – масштабируемое производство сложных электронных изделий, идущих в ногу с эволюцией компьютерных технологий.

На производстве работают квалифицированные сотрудники, которые решают задачи, требующие высокой точности действий и специальных навыков.

Исследования и разработки

Все ли идеи идут в производство и выводятся на рынок? Конечно, нет! Подразделение R&D в обязательном порядке проверяет жизнеспособность идей на прототипах. В компании перспективными разработками занимается целое подразделение. В таких исследованиях очень часто принимают участие не только опытные разработчики, но и даже студенты, которых привлекают для проверки новых идей.

Продукты и технологии

К 25-летию «Актива» портфель компании насчитывает более 100 продуктов и решений для защиты информации, среди которых системы для защиты и лицензирования ПО, программные и программно-аппаратные средства защиты информации, полностью отечественная линейка аппаратных продуктов и решений для аутентификации и создания электронной подписи, а также решения для защиты мобильных платформ. На протяжении последних двух лет компания производит более 2 млн электронных устройств ежегодно.

Флагманской разработкой компании является решение Рутокен ЭЦП 2.0. Это решение предназначено для строгой двухфакторной аутентификации и работы с электронной подписью. Рутокен ЭЦП 2.0 аппаратно поддерживает функции хеширования, вычисления электронной подписи и шифрования данных на неизвлекаемых ключах. Применяется в информационных системах с высокими требованиями к информационной безопасности: в дистанционном банковском обслуживании и электронном документообороте в государственном секторе и др.

Рутокен всегда прочно ассоциировался у партнёров и клиентов с электронной подписью, но сейчас Рутокен – это гораздо большее. Он позволяет внедрить строгую двухфакторную аутентификацию, решает проблемы несанкционированного доступа, помогает управлять парками токенов, смарт-карт и сертификатов.

Рутокен широко используется в комплексах защиты информации от НСД как средство двухфакторной аутентификации – базового защитного механизма, без которого невозможно функционирование систем НСД. Продукция Рутокен интегрирована в десятки лучших российских систем защиты от НСД.

Компания работает на стыке аппаратного и программного обеспечения. Есть железо, есть управляющий софт, которые пользователи видят на экранах своих компьютеров, планшетов и мобильных телефонов. «На борту» устройств работает собственная карточная операционная система Рутокен, включённая в Единый реестр российского ПО. Рутокен Плагин позволяет существенно расширить возможности устройств семейства Рутокен ЭЦП. При помощи плагина можно разрабатывать свои собственные системы и интегрировать функции двухфакторной аутентификации и электронной подписи в веб-приложения.

Везение или стратегия?

Чего больше в успехе компании? Руководители «Актива» считают, что без стратегии и без фокуса на достижении результатов долгосрочный успех невозможен в принципе. Но и везение тоже иногда хорошо помогает. Кто, например, 20 лет назад предполагал, что в государстве будет проводиться политика импортозамещения?

Так, принятые в начале 2000-х решения о разработке отечественных ключевых носителей для российского рынка дали возможность развивать целую отрасль. И сегодня во многом слова Рутокен и электронная подпись являются синонимами.

В заключение журнал CIS хочет пожелать руководству и всему коллективу «Актива» новых достижений, креативных идей и дальнейшего процветания!

Компания Актив

Компания «Актив» *– российский разработчик средств информационной безопасности, крупнейший в России производитель электронных идентификаторов, электронных ключей и решений для защиты программного обеспечения.*

www.rutoken.ru | www.guardant.ru

2014 – Смарт-карты
Компания вышла на рынок смарт-карт. Смарт-карты Рутокен ЭЦП поддерживают российские и международные стандарты.

2015 – Рутокен ЭЦП PKI
Рутокен для корпоративного рынка. Первый токен линейки Рутокен, сделанный на смарт-карточном чипе.

2018 – Guardant Sign SD
Проект Guardant, из которого выросла компания, живёт и развивается сейчас. Устройство с более производительным чипом имеет обновлённый корпус и извлекаемую flash-память в виде microSD-карты.

2019 – Рутокен ЭЦП 2.0 3000 type-C
Компания вывела на рынок первый сертифицированный токен с разъёмом USB Type-C. Теперь можно подписывать квалифицированной электронной подписью документы с Android-устройств.

Итоги благотворительной ИТ-конференции CISummIT «Digital Hearts»

CISummIT

Фонд Хабенского
CIS Современные Информационные Системы
СОВИНТЕГРА
TESSIS
gemalto security to be free
ORACLE
kaspersky
Единый портал Электронной подписи
SafeTech
IT-Events
skyeng

10 октября на площадке Digital October в Москве прошла первая благотворительная ИТ-конференция CISummIT «Digital Hearts», организованная журналом CIS «Современные Инфосистемы» в поддержку Фонда Константина Хабенского.

Концепция мероприятия

ИТ-конференция CISummIT «Digital Hearts» объединила самых активных участников ИТ-рынка, ведущих производителей и экспертов в сфере информационной безопасности, чтобы собрать средства для помощи детям с заболеваниями головного мозга.

Спикеры-практики, глубоко погружённые в тему, рассказали о своём видении современного ИТ-рынка, а также презентовали свои продукты и бизнес-решения на базе подробных теоретических подходов.

Гости мероприятия узнали самые актуальные и достоверные данные о новейших ИТ-решениях, в ходе общения завели деловые знакомства с партнёрами, зарядились энергией и отдохнули в приятной дружеской атмосфере.

Тематика мероприятия

В первой части ИТ-конференции CISummIT «Digital Hearts» выступили Иван Соковиков из компании Oracle и Игорь Афанасьев, представивший компанию THALES, Роман Жуков – «Гарда Технологии» и Екатерина Данилова из компании Kaspersky.

Во второй части свои доклады представили Анатолий Лебедев – доцент кафедры «Информационная Безопасность» МГТУ им. Баумана и Александр Чесалов, Кирилл Маркевич из компании «Системы практической безопасности», а также Роман Совалов – генеральный директор компании «Совинтегра».

В своих выступлениях спикеры раскрыли следующие темы:

- Обеспечение безопасности **облачных гетерогенных** сред
- Как доверять облакам, пользователям, вендорам и себе
- Дивный новый цифровой мир вокруг нас: зачем бизнесу на самом деле безопасность
- Как понять, кто пользуется вашим сервисом – лояльный клиент или мошенник
- Российские криптографические примитивы для IoT
- На пути к цифровому бессмертию
- Системы практической безопасности

Поездка редакции журнала и участниц «Мисс CIS» в лечебно-реабилитационный научный центр «Русское поле».

- Выполнение SLA ИТ-сервисов при реализации требований ИБ в условиях значимости качества каналов связи
- SAS для обеспечения двухфакторной аутентификации в корпоративных сервисах

Итоги и благодарности

Все спикеры отметили важность такого благотворительного мероприятия и с радостью выступали в нём.

Все докладчики были награждены памятными дипломами от генерального директора ООО «Современные Инфосистемы» Сергея Новикова и подарками от журнала CIS.

В конце дня состоялся фуршет, где в непринуждённой обстановке участники могли познакомиться и пообщаться друг с другом. Все собранные средства с мероприятия были перечислены в Благотворительный Фонд Константина Хабенского. Также была разыграна благотворительная лотерея, в которой мог принять участие любой желающий.

Благодаря участию спикеров и гостей ИТ-конференция CISummIT Digital Hearts помогла спасти ещё чью-то детскую жизнь и приумножить количество добрых сердец.

Редакция журнала будет рада видеть вас на следующих мероприятиях в числе наших гостей и участников.

CIS Современные Информационные Системы

CIS «Современные Инфосистемы» *– журнал об информационных технологиях в России.*

info@sovinfosystems.ru
www.cismag.ru


PKI Форум
Россия 2019
www.pki-forum.ru


CIS
Современные Информационные Системы


CIS


CIS


CIS


CIS

OTUS – продвинутые онлайн-курсы для ИТ-специалистов

- **Как вырасти из джуна до мидла за полгода?**
- **Что делать, если ты разработчик, который приуныл?**
- **Как разработчику добиться повышения зарплаты?**

Сегодня ИТ-рынок перегружен: из-за большого количества специалистов компаниям невыгодно бороться за них, предлагая больший размер зарплаты. Сейчас способных разработчиков всё больше «заманивают» другими условиями: бесплатным фитнесом, обедами и красивыми офисами. Из-за этого добиться повышения зарплаты в рамках одной должности сложно – нужен переход на более высокий уровень.

В наши дни для карьерного роста уже недостаточно просто отработать в компании несколько лет, читать много профессиональной литературы и проводить часы на GitHub. Нужно делать это системно: изучать статьи, которые подходят по специфике работы, брать в разработку код, который можно реально применить в будущей работе. Чтобы разобраться в этом самому, требуется много времени и сил.

Эту проблему решают онлайн-курсы OTUS – продвинутые курсы для профессиональных ИТ-разработчиков, на которых вы системно прокачаете свои навыки и за полгода дорастёте до новой позиции. Вот как это работает.

Как быстро повысить свой уровень

Главная причина застоя на позиции Junior – нехватка знаний. Зачастую непонятно, чего именно не хватает, чтобы расти дальше: теоретических знаний или практики. Начинаешь читать всё подряд, беспорядочно сёрфить GitHub и тратить кучу времени, чтобы найти что-то стоящее на YouTube.

В OTUS информацию дают системно и «по запросу»: не хватает знаний в Java – разберём синтаксис, расскажем, что происходит «под капотом», и вместе запустим проект. Никаких лишних занятий.

Например, студенты курса по алгоритмам учатся использовать структуры данных, работать с хеш-таблицами, графами, деревьями поиска, решать задачи динамического программирования. Всё это – навыки, необходимые Middle-разработчикам, которые хотят работать в крупных ИТ-компаниях вроде Яндекса или Microsoft.

До поступления на курсы OTUS я работал системным администратором Windows в разных проектах в течение 8 лет. На последнем месте работы достиг позиции Senior и приуныл: с завистью смотрел на админов Linux, на DevOps-инженеров, которые могли работать удалённо и зарабатывать в 2-3 раза больше.

Сначала пробовал проходить курс в одной известной онлайн-школе, но меня очень разочаровал процесс. Это правда было ужасно: преподаватели, которые не могли внятно ответить на вопросы и не знали сути преподаваемого предмета. Где-то в сети я наткнулся на курс OTUS «Администратор Linux» (тогда был первый набор). И он мне понравился: там действительно разбирали интересные вещи и уделяли внимание деталям.

В итоге, в середине обучения я получил работу Linux-администратора в компании, занимающейся поддержкой Linux-серверов.

Павел Козлов, выпускник OTUS

А зарплата точно вырастет?

Возможно, не сразу, но в перспективе вы точно сможете рассчитывать на повышение. Во-первых, вы будете изучать только то, что действительно пригодится для работы. Например, начинающий Data Scientist не сильно отличается от других Junior-разработчиков и получает от 80000₽, а тот, кто закроет все пробелы в знаниях математики, сможет за 4-5 месяцев выйти на уровень оплаты выше 150000₽.

Если до обучения специалист способен заниматься только базовыми вещами, то после он готов сразу идти в бой, например самостоятельно реализовать REST API для приложения.

Во-вторых, по окончании обучения вам будет что показать работодателям: каждый студент презентует выпускной проект по теме курса. Это отдельная работа, на выполнение которой отводится последний месяц обучения.

На первой работе Linux-администраторам платили так же, как и на позиции Windows. Но через 3 месяца я уже работал DevOps-инженером и занимался развёртыванием и поддержкой облачных решений, CI/CD инструментов и созданием счастливой жизни для разработчиков. При этом зарплата у меня была уже выше, чем раньше. Впереди было ещё много часов чтения книг, документации, прохождения курсов – всё это помогало осваивать новые технологии и становиться классным и нужным специалистом.

Павел Козлов, выпускник OTUS

А есть гарантия, что это поможет?

Успешные выпускники – это и есть гарантия качества курсов. Ещё до окончания обучения лучшие студенты получают приглашение на собеседование в компании-партнёры OTUS – СберТех, Яндекс, IBS, Ozon, Avito, Nvidia, Газпромбанк и другие.

Ну а те, кому оффер не сделали, всё равно будут в поле зрения HR-специалистов: OTUS-комьюнити поможет найти работу как можно быстрее.

Сегодня я работаю системным инженером в компании, занимающейся разработкой софта: интересные задачи, высокая зарплата, удобный график. К этому я пришёл за 2-3 года. Если бы OTUS мне попался раньше и я не был бы таким жадным (курсы в любом случае окупаются, но понимание об инвестициях в себя приходит не сразу), путь был бы короче. В планах попасть на курс «Инфраструктурная платформа на основе Kubernetes».

Павел Козлов, выпускник OTUS

Что ещё нужно знать?

Занятия в OTUS проходят онлайн – два-три раза в неделю по вечерам в течение 4-5 месяцев. Это значит, что от текущей работы отказываться не придётся. А если вы пропустите вебинар, можно будет посмотреть его запись и задать уточняющие вопросы лично куратору.

Оплатить можно как сразу, так и частями, есть также возможность оплаты в кредит. Для поступления на курс студенты проходят онлайн-тестирование. Посмотреть, что в него входит, можно на сайте. Если вы новичок в OTUS, в течение 7 дней после регистрации для вас будет действовать скидка 4000 рублей на любой курс.

OTUS

***Otus.ru** – высокотехнологичный стартап в области образования. Наша миссия – делать обучение осмысленным, реализуя взаимосвязь между ожиданиями работодателей, компетенциями специалистов и возможностями преподавателей. Мы не обучаем основам, а предлагаем углубленные знания.*

www.otus.ru

«Спасательный ИТ-круг» для рынка электронной подписи

Уже сейчас можно констатировать, что 2019 год для российских удостоверяющих центров (УЦ) выдался непростым. Длительное отсутствие необходимых законодательных изменений в рассматриваемой области (ужесточение требований к аккредитуемым УЦ, регулирование облачной подписи, реформа технологии применения электронной подписи (ЭП) при подписании электронных документов и т. д.), стало основной причиной активизации мошенников.

Определившие «узкие места» и адаптировавшиеся к текущим методам защиты преступники развернули свою деятельность во всех регионах России. Об этом свидетельствуют многочисленные новости, статьи и репортажи о пострадавших, наполнившие средства массовой информации. При помощи выпущенных без ведома владельцев ЭП мошенники чаще всего регистрировали компании на ничего не подозревающих граждан, а затем брали кредиты/незаконно возвращали НДС и т.д.

Справочно: При создании электронной подписи УЦ по поручению заявителя генерирует ключ электронной подписи и ключ проверки электронной подписи.

Представители контролирующих органов подняли вопрос **о кризисе отрасли ЭП** и необходимости государственной монополизации выпуска квалифицированных сертификатов для юридических лиц путём передачи права их изготовления в УЦ ФНС России. Но массовость и частота использования электронных подписей в бизнес-процессах, а также технологическая сложность эксплуатации и высокая стоимость оборудования для генерации не позволят «по щелчку пальцев» переориентировать рынок.

«Спасение утопающих – дело рук самих утопающих»?

Несмотря на обозначенные проблемы, неопределённо длительное время* удостоверяющие центры продолжат закрывать потребность «федерального масштаба» в ЭП, обеспечивая сертификатами юридических и физических лиц. Но в изменившихся реалиях придерживаться прежних бизнес-моделей **слишком рискованно**.

Задача, стоящая перед рынком, – вернуть взаимное доверие между УЦ и их клиентами, нейтрализовав образовавшиеся бреши в законодательном регулировании использования ЭП и минимизировав возможный ущерб для добросовестных участников информационного взаимодействия. Для её решения Госкорпорация «Ростех» с группой компаний

* Статья подготовлена в конце октября 2019 года, все свежие законодательные изменения представлены на Едином портале Электронной подписи.

«Селдон» подписали меморандум о создании **удостоверяющего центра «Основание»**, который бросит «спасательный ИТ-круг» участникам рынка, находящимся по обе стороны от программно-аппаратного комплекса генерации ключевой пары.

В основу удостоверяющего центра положено типовое решение, основные компоненты которого:

- центр сертификации, предназначенный для формирования сертификатов ключей проверки ЭП пользователей и администраторов УЦ, для создания и хранения списков аннулированных сертификатов;
- центр регистрации, хранящий данные, запросы на сертификаты и сертификаты клиентов, представляющий интерфейс для взаимодействия пользователей с УЦ;
- автоматизированное рабочее место администратора – точка регистрации пользователей, формирования служебных ключей и сертификатов пользователей, управления центром регистрации.

Справочно: Программно-аппаратный комплекс (ПАК) объединяет компоненты УЦ в единую систему, обеспечивая их работоспособность.

Удостоверяющий центр «Основание» аккредитован Министерством цифрового развития, связи и массовых коммуникаций РФ. В работе УЦ использует сертифицированный по требованиям ФСБ России ПАК и защищённую по требованиям ФСТЭК России информационную среду.

Базовая модель удостоверяющего центра дополнена **инновационной ИТ-системой**, позволяющей эффективно управлять компанией, контролировать её бизнес-процессы и оперативно подключать новых партнёров к выпуску электронной подписи. ИТ-разработка уделяет особое внимание качеству идентификации получателей ЭП, что является необходимым элементом для восстановления среды взаимного доверия на рынке.

Благодаря интеграции со СМЭВ и её сервисами (МВД, ПФР, ФНС), а также автоматизации всех законодательно допустимых участков, ИТ-система позволяет максимально контролировать выпуск электронных подписей, сводит к минимуму возникновение ошибок, связанных с человеческим фактором, а также позволяет тратить минимальное количество времени на оказание услуг клиентам, обратившимся в УЦ (точку выдачи).

Для успешной надстройки ИТ-системы команда УЦ объединила опыт Ростеха по внедрению новых цифровых сервисов в рамках национального проекта «Цифровая экономика» и опыт разработки ИТ-решений ГК «Селдон», полученный во время реализации ряда крупнейших проектов для коммерческих организаций и государственных ведомств.

Коллаборация компаний призвана внедрить новую бизнес-модель удостоверяющего центра и спасти региональных участников рынка, которые не в силах самостоятельно справиться с вызовами современной цифровой среды. Обозначенный регулятором кризис доверия, потребность клиентов в максимальной скорости оказания услуги при условии сохранения качества и обеспечения должного уровня безопасности – все эти **проблемы помогает минимизировать разработанная УЦ «Основание» ИТ-система**.

Предложенное командой удостоверяющего центра решение – одно из наиболее свежих на рынке, использованные при его создании современные технологии позволяют гибко дорабатывать функционал. Так, помимо брендирования личного кабинета под индивидуальный стиль, по просьбам партнёров разработчики внедрили обучающий инструментарий.

«Шире круг»

В настоящее время УЦ «Основание» активно формирует партнёрскую сеть из компаний, которые делают свой выбор в пользу надёжности, технологичности и готовности оставаться на рынке и после законодательного ужесточения требований к удостоверяющим центрам. Важным условием совместной работы является наличие лицензии ФСБ России у будущей точки выдачи либо готовность компании её получить при посредничестве специалистов УЦ «Основание».

Почему только лицензиаты?

Действующее законодательство в сфере использования ЭП допускает работу в качестве доверенных лиц аккредитованных УЦ партнёров (точек выдачи) без лицензии ФСБ России, в случае если их деятельность не составляет лицензируемый вид деятельности (изготовление ключей ЭП, распространение и обслуживание средств криптографической защиты информации (СКЗИ) и т.д.). Основным направлением работы таких нелицензированных точек выдачи является проверка документов клиента. Однако на практике подобные партнёры зачастую не отказываются и от генерации ключей ЭП, и от продажи средств ЭП.

Стремление охватить как можно большую часть рынка за счёт построения широкой партнёрской сети может вести аккредитованный УЦ к заключению договоров с «практически любым желающим», что без сомнения сказывается на уровне безопасности. При подобном сценарии в случае выпуска сертификата без ведома его владельца следы преступления часто теряются в точке выдачи. В то же время удостоверяющим центром договор с недобросовестным партнёром расторгается и заключает новый с аналогичным индивидуальным предпринимателем или юридическим лицом.

Соответствие требованиям регулятора говорит о том, что понимание принципов организации системы информационной безопасности и ответственности у лицензиата находится на должном уровне. Партнёрская сеть удостоверяющего центра «Основание» формируется исключительно из компаний и индивидуальных предпринимателей, имеющих или готовых получить лицензию ФСБ России.

Узнать подробнее о том, как присоединиться к кругу партнёров удостоверяющего центра «Основание», можно, отправив название компании или ИП и контактные данные на почту partners@iecp.ru.

Объединение региональных участников, формирование общих стандартов, позволит сформировать УЦ, готовый обеспечить качество и надёжность оказываемых услуг.

Основание
Удостоверяющий центр

Удостоверяющий центр «Основание»

uc-osnovanie.ru

8-800-511-70-50

partners@iecp.ru

7 этапов эволюции тестирования в компании

Статья будет интересна ИТ-директорам, менеджерам по продукту, менеджерам проектов и всем, кто хочет лучше разобраться в процессах обеспечения качества проектов.

Иван Бормотов,
руководитель агентства тестирования Qualitica и аутсорс-продакшена Кодеры

В Qualitica мы тестируем большие веб и мобильные проекты как частные, так и государственные. До появления отдельного агентства тестирования 10 лет в качестве специалиста и руководителя нескольких digital-студий я наблюдал, как в разных компаниях тестирование зарождается, растёт и становится отдельным важным направлением деятельности. Обычно в любых ИТ-проектах (сайты, приложения, игры, корпоративное ПО) начинают с отношения к тестированию как к формальной процедуре. Но с ростом уровня проектов эволюционирует и тестирование: в нём участвует больше людей, а процессы становятся сложнее.

Я выделил 7 ключевых стадий эволюции тестирования, чтобы проиллюстрировать, как меняются подходы к обеспечению качества в компаниях. Разработчики смогут проследить эволюцию тестирования, определить свой текущий этап и узнать, что стоит предпринять для улучшения процесса и качества тестирования.

1. Нет тестировщика. Его функции выполняет сам разработчик или менеджер.
2. Тестировщики появляются, но тестируют проекты только на стадии завершения.
3. Тестировщики проверяют все задачи разработчиков на предмет соответствия результата изначальной постановке задачи.
4. Тестировщики занимаются тест-дизайном.
5. Внедряется система управления тестированием.
6. Появляется автоматизация тестирования.
7. Усложняется иерархия, появляются новые роли в команде тестирования.

Теперь о каждой стадии подробнее.

Стадия 1. Тестирование выполняет разработчик и\или менеджер

«Сделал – проверь за собой» – самый простой «инстинктивный» подход к тестированию. Обычное дело в небольших компаниях. Когда нет возможности нанять профессионального тестировщика или нет понимания необходимости тестирования, этот фронт работ выполняется своими силами. Тестировать самому – самый нерациональный и проблемный подход. И вот почему:

- Сам разработчик тестирует только те сценарии, которые реализовал, и с теми данными, которые использовал в процессе разработки. При таком тестировании «в вакууме» альтернативные сценарии опускаются. В итоге жизнь вносит коррективы, и у конечных пользователей, как правило, всплывают ошибки.
- Если тестирует менеджер, то он делает это в качестве дополнительной нагрузки, не владея экспертизой и не имея времени и моральных сил плотно заниматься тестированием. Так можно обнаружить грубые ошибки, но многие нюансы упускаются из виду.
- Субъективное отношение к проекту, желание побыстрее его сдать ведут к соблазну закрыть глаза на ряд, казалось бы, «несущественных» проблем.

Крайний случай, когда тестированием в компании вообще не занимаются, а репорт об ошибках приносит заказчик. Он получил релиз, всё уже на боевой среде, разработчик отчитался о запуске. Клиент открывает проект и видит какую-то банальную ошибку базы данных или ошибку сервера. Потом ещё и ещё ошибки. Клиент становится тестировщиком за свои же деньги.

Стадия 2. Тестировщик проверяет проект в самом конце

Проверить весь проект на предрелизной стадии – классический метод при работе по модели Waterfall. Проект разделяется на глобальные этапы (иногда весь проект это один этап). На каждом этапе сначала делается софт, а уже потом тестируется. Тестирование уже есть, и это хорошо. Но проблемы тоже есть, и совершенно конкретные.

Во-первых, когда мы тестируем в самом конце, серьёзные ошибки на уровне архитектуры будут найдены слишком поздно. Потребуется переделывать большую часть, а то и весь проект. Это никому не выгодно.

Во-вторых, при отсутствии документации мы можем провести только поверхностное тестирование методом свободного поиска. Это сразу выключает часть альтернативных сценариев. Бывает, что документация есть, но в процессе задачи видоизменяются, и готовый продукт отличается от картинки на бумаге. Опять же возникают сложности в тестировании и в разборе баг-репортов.

В третьих, практически всё время проекта обычно закладывается на разработку как приоритетную задачу. Оставляют немного времени на проверку. А вот на исправление ошибок времени-то и нет, порой внушительные доработки тормозят проект и срывают сроки.

При раздельном тестировании этапов возникает другая проблема. Между этапами тестировщик забывает детали проекта, и ему приходится каждый раз вникать в происходящее. Это тоже трата рабочих часов.

В общем, проверять проект в самом конце логично и вроде бы правильно, но этот метод не учитывает риск обнаружения глобальных ошибок. Поэтому тестирование эволюционирует дальше.

Стадия 3. Все задачи проверяются на соответствие результата изначальной задаче

Далее компания понимает, что лучше отлавливать ошибки по мере их накопления. Стало быть, переключаемся с Waterfall-модели на методологию Agile. В этот момент тестировщиков более тесно интегрируют в процесс разработки. Все задачи начинают последовательно многократно тестироваться: отдельно, в составе релиза, на боевой среде.

На этой стадии задачи проверяются на соответствие заявленным требованиям. Agile помогает работать лучше, но далеко не все тестировщики, и особенно их руководители готовы по-новому относиться к тестированию.

Руководитель ждёт от тестировщиков скорости и качества, а понимания необходимости тестовой документации и проведения регрессионного тестирования ещё нет. Отсюда типичные проблемы этой ступени эволюции.

Тестирование проводится больше интуитивно, чем структурированно. Главенствует принцип: «Что вижу, то и тестирую». При каждой итерации делаются разные проверки и в разной последовательности. В результате ошибку можно как минимум пропустить на одном из этапов тестирования или вообще не увидеть. Альтернативные сценарии и изменения в связанном функционале тоже могут выпасть из поля зрения.

Плюс проблема с регресс-тестированием, которое если и проводится, то бессистемно. По факту тестировщик проверяет то, что сам считает нужным или то, что ему посоветовал проверить разработчик/менеджер.

Стадия 4. Тестировщики занимаются тест-дизайном

На этой стадии на сцену выходит тест-дизайн. Тестировщики начинают осознанно уделять внимание анализу требований. Функционал разбивается на логические блоки, которые покрываются чек-листами или тест-кейсами.

Чек-лист – список проверок, необходимых для тестирования функционала. Чек-листы более распространены, так как их проще поддерживать в актуальном состоянии, особенно в рамках большого динамичного проекта.

Тест-кейс – последовательность шагов, которые необходимо пройти для проверки функционала. Описание каждого шага сопровождается указанием на ожидаемое поведение системы.

Появляется полноценная **тестовая документация,** по которой можно отследить, как проверяется тот или иной функционал. Тестовая документация полезна не только при первичном тестировании, но и в регрессионных тестах.

Всё это и называется тест-дизайном. Можно сказать, что на этой стадии начинается осмысленное профессиональное тестирование. Больше это не просто гора задач, которые нужно проверить, а структурированный процесс по анализу требований, формированию тестовой документации и непосредственному тестированию. В том числе меняется подход к тестовым данным. Данные уже не придумываются спонтанно в процессе, а берутся из заранее подготовленных наборов.

Явных минусов на стадии тест-дизайна нет. В целом это уже достойный уровень тестирования. Для потокового производства сайтов или подобных проектов тест-дизайна более чем достаточно. Главное, правильно подходить к процессу тестирования: проанализировать продукт, составить документацию и по ней провести тесты.

Стадия 5. Внедряется система управления тестированием

Далее компания дорастает до необходимости использования специализированных систем для хранения тест-кейсов (чек-листов) и выполнения тестовых прогонов.

Такая система позволяет:

- хранить требования и тест-кейсы;
- связывать требования с тест-кейсами;
- анализировать тестовое покрытие;
- хранить разные версии тест-кейсов;
- выполнять тестовые прогоны;
- проводить сравнительный анализ по тестовым прогонам;
- вести отчётность по тестированию;
- отслеживать рабочую нагрузку команды для корректировки задач и ресурсов.

Система – это всегда новая ступень эволюции. В нашем случае прежде всего улучшается контроль за процессом тестирования. Мы лучше управляем тестами и получаем новый уровень качества продукта.

На поздних стадиях развития проекта такая система помогает всем участникам помнить, как вообще что-то должно работать и как это проверять. Система ускоряет ввод в проект новых участников.

Стадия 6. Автоматизируются регулярные проверки

В процессе длительного развития проектов возникает потребность автоматизировать отдельные проверки. Для этого разработчики и тестировщики пишут автотесты. Разработчики обычно делают unit-тесты, тестировщики – ui-тесты. Начинают с покрытия автотестами позитивных сценариев использования ключевого функционала: авторизации, регистрации, публикации записей и тому подобное.

Разработанные автотесты включаются в процесс непрерывной интеграции (CI/CD), что позволяет команде узнавать об ошибках непосредственно в момент коммита.

Автотесты значительно сокращают расходы на регрессионное тестирование и повышают качество конечного продукта. Но, чтобы их делать, нужен определённый уровень тестировщика. Также стоит знать, что автотесты не имеет смысла делать на ранних стадиях проекта. Система быстро меняется, поэтому во избежание фантомных ошибок нужно менять и автотесты, что занимает время.

Стадия 7. Усложняется иерархия, появляются новые роли

Мы подошли к высшей стадии эволюции, когда в отделе тестирования значительно усложняется иерархия и появляются узкие специалисты: тест-менеджер, тест-лид, тест-аналитик, тест-дизайнер и так далее.

Команда растёт, задачи усложняются. Например, **тест-менеджер** больше всех знает о продукте и занимается организацией тестирования на более высоком уровне. Он чаще и более тесно коммуницирует с заказчиками и разработкой, нежели с командой тестирования.

Тест-лид организует тестирование на проекте и распределяет задачи внутри команды. **Тест-аналитик** занимается аналитикой требований, их декомпозицией и приоритезацией, готовит материал для тест-дизайна и последующего тестирования. А **тест-дизайнер** трансформирует требования в чек-листы и тест-кейсы.

Новые роли нужны на больших проектах, где работает целая команда тестировщиков. Появление подобных ролей ведёт к ещё большей структуризации процесса тестирования, без чего невозможна работа над большими и сложными ИТ-проектами.

Выводы

Мы рассмотрели ключевые стадии эволюции тестирования в компании. Осознанное профессиональное тестирование начинается со стадии тест-дизайна. Тест-дизайн даёт устойчивое повышение качества продукта.

Процесс развития тестирования не всегда линейный. Вы можете пропускать, объединять, смешивать определённые этапы или сразу выходить на более высокий уровень. Например, у нас в Qualitica есть система управления тестирования, то есть мы на стадии 5. Сейчас практически одновременно у нас появляются узкие специалисты (новые роли, стадия 7) и автоматизация (стадия 6).

Далеко не всем и не всегда нужны система управления тестированием, автотесты и тем более тест-дизайнер. Но, оставаясь на этапе инстинктивного тестирования или ограничиваясь финальными проверками, делать сложные длительные проекты вряд ли получится. Поэтому желаю вам найти нужную точку в процессе развития тестирования и прийти к ней, чтобы повысить качество тестирования и давать заказчикам продукт высокого качества.

Об авторе

Иван Бормотов – руководитель агентства тестирования Qualitica и аутсорс-продакшн Кодеры рассказал о 7 стадиях эволюции тестирования в компании разработки. С 2009 по 2015 годы Иван работал в агентстве Notamedia (в том числе на позиции директора по развитию), руководил проектной командой по разработке больших ИТ-проектов для Правительства Москвы и Московской области. Основал аутсорс-продакшн DigitalWand, который по итогам 2018 года признан № 1 на рынке аутсорс-разработки по версии Tagline.

Конкурс красоты «Мисс CIS» 2019

Красота, пожалуй, одна из самых субъективных и переменчивых категорий. То, что ещё несколько лет назад считалось эталоном женской привлекательности, сегодня уже не является таковым.

Но не стоит забывать, что представление о женской красоте у всех людей разное. И именно благодаря этому факту каждый человек может найти свою идеальную вторую половинку.

Вот почему для современной женщины так важно научиться любить и принимать себя такой, какая она есть, без условий и ограничений.

О конкурсе

Всероссийский ежегодный конкурс красоты, организованный редакцией журнала CIS (Современные Информационные Системы), прошёл 9-го ноября в уютной камерной атмосфере элегантного ресторана «Светлый» в городе Москве.

В конкурсе приняло участие 25 девушек из разных городов России, работающих в сфере информационных технологий и информационной безопасности.

Праздник открыл торжественный гала-ужин, посвящённый конкурсу красоты «Мисс CIS». На протяжении всего мероприятия праздничное настроение гостей и участниц поддерживала специально приглашённая музыкальная группа JukeBox – акапельное трио, выступающее в своём собственном стиле, сочетающем техники акапеллы и битбокс. Кульминацией шоу-программы стало завораживающее шоу с жидким азотом и фокусами, а на этапе вручения короны победительнице на сцену обрушился дождь из золотого конфетти!

История создания

Прежде чем продолжить, сделаем небольшой экскурс и расскажем о предыстории конкурса.

А началось всё с того, что около года назад в редакции журнала CIS провели увлекательный эксперимент. В ходе закрытого голосования мужчинам предложили выбрать исключительно по своему субъективному мнению 10 лучших участниц одного из конкурсов красоты.

Оказалось, что мужчины абсолютно по-разному оценили победительниц. В качестве главных критериев отбора мужчины ориентировались на яркость девушки, спортивность, скромность, модельную внешность, а для кого-то приоритетом стала схожесть интересов.

Кстати, главный редактор на 100% был уверен в победе одной из конкурсанток, которую сразу выделил среди других участниц. В то время

как остальные мужчины не удостоили эту девушку даже десятки лучших! Что это значит? А то, что все девушки конкурсантки по-своему прекрасны, и итоги конкурсов красоты – это лишь субъективные предпочтения действующих членов жюри.

Эксперимент настолько увлёк редакцию ИТ-журнала CIS, что было принято решение организовать собственный всероссийский конкурс красоты, а заодно развеять устойчивый миф о том, что в сфере ИТ девушкам не место, а уж тем более красивым.

Так и появился конкурс красоты «Мисс CIS» среди девушек, работающих в сфере информационных технологий и информационной безопасности по всей России.

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

Финальное торжество

Как и обещали организаторы, финальное торжество оказалось ярким и запоминающимся. И участницы, и приглашённые гости получили массу приятных впечатлений.

Отдельно выражаем огромную благодарность многоуважаемым жюри, экспертам в сфере ИТ-технологий и, безусловно, женской красоты.

А жюри выступили:

- Юрий Маслов – коммерческий директор компании «КриптоПро».
- Максим Щеглов – компания «ТрансТелеком».
- Денис Горчаков – директор по кибербезопасности рекламного холдинга.
- Ефремов Роман – руководитель направления Управление информационной безопасности СБ.
- Сергей Новиков – генеральный директор журнала «CIS – Современные информационные системы».
- Лев Шумский – директор по информационной безопасности Ассоциации ФинТех.
- Станислав Гонтаренко – директор по информационной безопасности компании «Мандарин».
- Горбачёв Евгений – начальник отдела противодействия киберугрозам АО «Газпромбанк».
- Лебедев Анатолий – профессиональный российский криптограф, доцент кафедры Информационной безопасности МГТУ им. Н.Э. Баумана, «крёстный отец» криптографических стандартов Республики Беларусь.
- Павел Клепинин – генеральный директор Цифрум «Росатом».

Вечер завершился награждением победительниц конкурса, которых выбрали почётные члены жюри.

Главный титул **«Мисс CIS»** завоевала прекрасная москвичка Анастасия Колоскова. Девушка занимает должность менеджера по работе с клиентами в компании «Тайгер Оптикс». Увлекается бодибилдингом и живописью.

В анкете Анастасия поделилась интересным фактом из своей жизни: 6 лет она работала тренером по бодибилдингу, после чего резко сменила область деятельности и около года проработала бортпроводником, но в итоге ушла в ИТ-сферу. Мечта Анастасии – стать CISO.

На вопрос: «Почему именно Вы должны стать «Мисс CIS»?» девушка ответила: «Я спортсменка и привыкла ставить перед собой цель – победить!»

Анастасия достигла своей цели, с чем мы её и поздравляем!

1-й Вице «Мисс CIS» стала Валерия Голубкова-Ягодкина – специалист по отраслевым RFID-решениям компании «АйТиПроект» город Москва.

Валерия любит спорт и обожает путешествовать. А ещё девушка пишет короткие юмористические тексты.

Мечта 1-й Вице «Мисс CIS» – сидя на берегу океана с бокалом вина, думать о глобальной цифровизации! Идеально, правда?

2-й Вице «Мисс CIS», по мнению нашего почётного жюри, стала Елена Титович. Девушка занимает важный пост коммерческого директора в компании Headtechnology в городе Москве. Любит путешествовать, а в свободное время увлекается визажем.

Елена очень целеустремлённая и трудолюбивая девушка. Училась и больше года работала в Канаде. А 8 лет назад переехав в Москву, она самостоятельно построила успешную карьеру.

Мечта Елены – отправиться в кругосветное путешествие. Желаем, чтобы мечта как можно скорее воплотилась в жизнь!

Не остались без внимания и остальные участницы «Мисс CIS» 2019. В течение конкурса девушки проходили серию мастер-классов, где продемонстрировали многочисленные таланты и были отмечены почётными номинациями. Итак…

- Победительницами в номинации **«Мисс Кулинария»** стали Татьяна Зверева и Анастасия Колоскова.
- Звание **«Мисс За рулём»** в честной борьбе получила Ирина Василевская.
- В номинации **«Мисс Ювелир»** победила Ирина Налётова.
- Титул **«Мисс Вдохновение»** завоевала Анастасия Колоскова.
- **«Мисс Журналистика»** стала Ирина Налётова.
- В номинации **«Мисс Милосердие»** победили девушки с добрыми сердцами Анастасия Колоскова и Валерия Голубкова-Ягодкина.
- А одну из самых почётных номинаций **«Мисс Зрительских симпатий»** получила очаровательная Елена Титович.

Призы и подарки

Всем участницам конкурса были вручены многочисленные памятные призы и ценные подарки. Девушки получили ювелирные украшения, гаджеты, подарочные сертификаты, дипломы и, конечно, цветы.

Самого ценного и почётного подарка была удостоена победительница. Она получила роскошную корону, созданную специально для конкурса «Мисс CIS» 2019 брендом ювелирных украшений EFREMOV.

Всероссийский ежегодный конкурс красоты, организованный редакцией журнала CIS, состоялся! Это был удивительный феерический праздник красоты и грации. В следующем 2020 году мы ждём новых красивых и талантливых участниц из сферы информационных технологий и информационной безопасности, чтобы вновь выбрать самую достойную. До новых встреч!

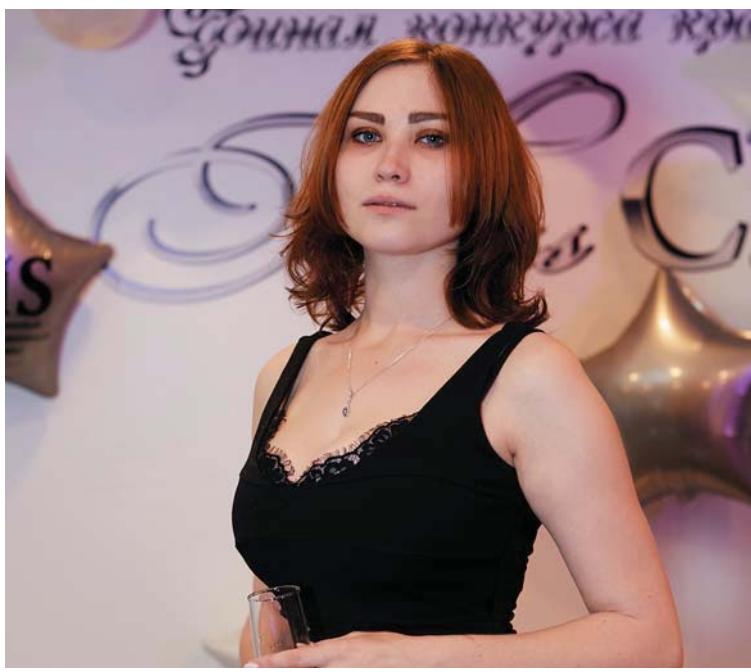

Мисс CIS
2-я Вице-Мисс
CIS 2019
2-я Вице-Мисс CIS 2019


CIS


3
CIS


Мисс CIS • 2019


1-я Вице-Мисс




Мисс CIS
ДИПЛОМ
Мария
Усачёва


CIS


13


Мисс CIS
ДИПЛОМ
Дарья
Коваленко
CIS


Мисс CIS
CIS

«Тайгер Оптикс»

Анастасия Колоскова
Tiger Optics. Cyber Security Distributor

О компании

Компания **«Тайгер Оптикс»** была основана в 2010 году и является специализированным дистрибьютором инновационных решений в сфере **информационной безопасности**.

Мы помогаем компаниям снижать риски, связанные с информационными технологиями, и защищать данные на всём протяжении корпоративной инфраструктуры: от дата-центра до конечных точек – рабочих станций, удалённых офисов и мобильных устройств.

За время работы Тайгер Оптикс впервые вывел на рынки России, Украины, Казахстана и других стран СНГ такие бренды, как Senetas, VMware AirWatch, Good Technology, Palo Alto Networks, TIBCO LogLogic, «Аванпост» и другие.

Тайгер Оптикс работает на всей территории русскоязычной Восточной Европы и Центральной Азии, осуществляя продажи и оказывая техническую поддержку через сеть авторизованных партнёров.

Основы работы компании

Тайгер Оптикс проводит тщательный анализ и тестирование решений и работает только с теми производителями, которые понимают насущные потребности заказчиков и создают соответствующие решения. Поэтому предлагаемые нами продукты – это лидеры инноваций рынка информационной безопасности.

В основе функционирования компании лежат четыре принципа:

- Портфель **актуальных решений,** тщательный отбор **лучших вендоров**
- **Наивысшие стандарты** клиентского обслуживания в отрасли
- **Высокая компетентность** и постоянное развитие сотрудников
- **Поддержка и защита партнёров** – реселлеров и системных интеграторов

Политика компании

Наш стандарт – объективность и профессионализм. Мы стремимся быть **стратегическим партнёром** заказчика, к которому обращаются не только для покупки продукта, но и за советом и консультацией. Мы стремимся к чёткому формулированию целей и задач клиента и только затем переходим к подбору оптимальных решений для их реализации.

Наши главные ценности – клиенты и сотрудники. Сотрудникам компании обеспечены все условия для профессионального роста и развития. Организовано участие в ежегодных тренингах, программах обучения и сертификации, затрагивающих как технические квалификации, так и лидерские качества, и умение эффективно коммуницировать информацию.

Наше преимущество – лидирующие инновационные продукты. Мы не поставляем «сырые» решения, равно как и устаревшие продукты, продвигаемые под видом новых «модных» технологий. Мы гордимся работой с лидерами рынка информационной безопасности.

ТАЙГЕР ОПТИКС

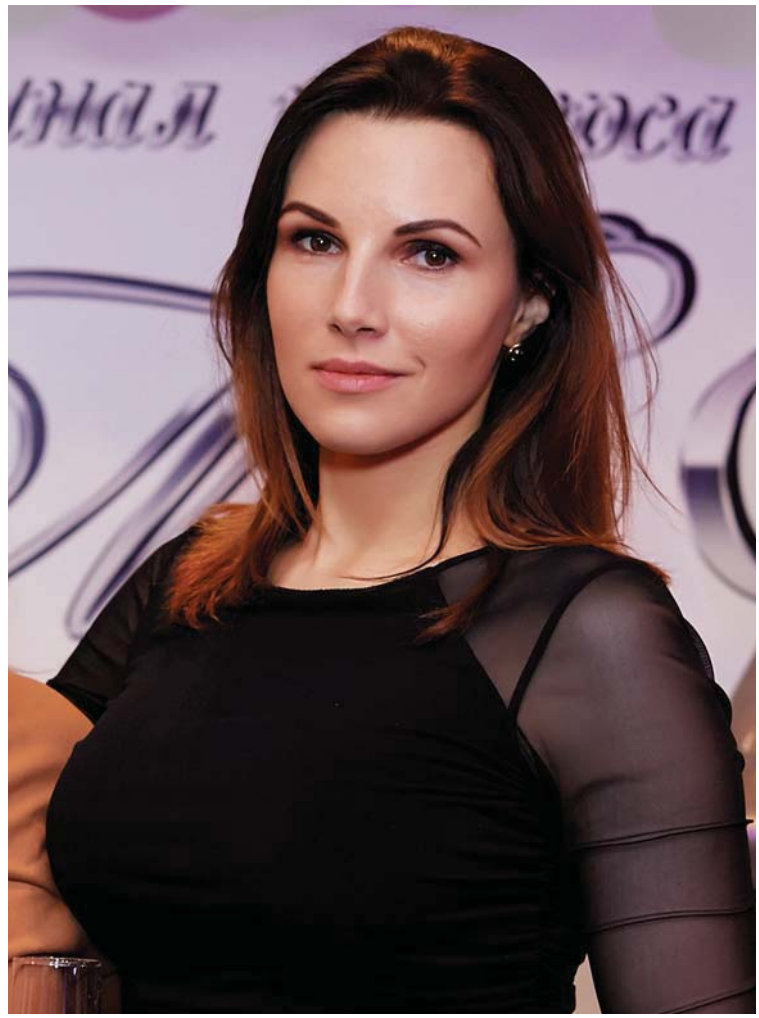
«Тайгер Оптикс» — является специализированным дистрибьютором инновационных решений в сфере информационной безопасности.

www.tiger-optics.com

«АйТиПроект»

Кто я? Я – Голубкова-Ягодкина Валерия, специалист по отраслевым RFID-системам компании «АйТиПроект».

Если театр начинается с вешалки, то практически любой проект нашей компании начинается с меня: от первого «Здравствуйте» до последнего подписанного документа приёмо-сдаточных работ. Каждый проект – это большая командная работа, где задействованы все специалисты нашей компании.



Валерия Голубкова-Ягодкина
Компания «АйТиПроект»

Кто мы? Мы – компания «АйТиПроект», ведущий российский разработчик и интегратор систем на основе технологии радиочастотной идентификации (RFID), работающий в сфере информационных технологий с 2004 года.

Для того чтобы подробнее рассказать о нашей деятельности, нужно познакомить читателя с самой технологией RFID и дать определение основным элементам системы.

Что такое RFID

RFID (англ. Radio Frequency Identification – радиочастотная идентификация) – способ автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах, или RFID-метках. Технология предполагает использование радиоволн определённой частоты для считывания, захвата и передачи информации. Этим RFID отчасти напоминает идентификацию типа «свой-чужой», используемую в военной сфере. Собственно, оттуда технология и берёт своё начало. Первые чипы, работающие на современном принципе радиочастотной идентификации, были представлены и испытаны в 1973 году, а спустя 15 лет технология уже была достаточно хорошо отработана и запатентована.

Суть работы RFID-систем во взаимодействии двух основных составляющих элементов – метки (или тэга) и приёмника – считывающего устройства. Пассивный элемент – метка (чип) – предназначен для хранения информации, а активный – считыватель (терминал) – необходим для считывания этих данных путём радиочастотного взаимодействия. Таким образом можно легко идентифицировать объекты на расстоянии без непосредственного контакта с ними, что, например, необходимо при считывании штрих-кода или QR-кода.

Работает вся система следующим образом: считыватель (сканер) генерирует электромагнитное поле, а метка принимает эти волны, преобразуя их в сигнал и в электроэнергию, используемую для питания самого чипа. Полученная энергия необходима для выполнения определённых действий – генерации и отправки обратного сигнала, который принимает уже сканер. При электромагнитном воздействии на метку возможно не только считывание с неё информации, но и запись данных.

Взаимодействие между меткой и сканером может осуществляться на разных радиочастотах, быть одноразовым или многократным. Сигнал также может шифроваться для дополнительной защиты информации от считывания мошенниками. Сфера применения и характеристики работы системы зависят от конструктивных особенностей самого чипа (метки).

RFID-метки. Различаются разные виды меток, в частности универсальные или строго для металлических объектов в виде наклеек, бирок, брелоков, браслетов или этикеток. Есть различия в устройствах в зависимости от используемой памяти (одноразовая запись, с возможностью многократного чтения, с правом записи другой информации). Существуют **активные и пассивные метки.** Первые способны работать на значительно большем расстоянии, поскольку у них есть свой источник питания. У пассивных меток источника энергии нет. Существует также такой вариант устройств, как полупассивные метки. Они работают по тому же принципу, что и пассивные, но оснащены батареей для питания чипа.

Одним из ключевых определений RFID-системы является такой показатель как частота или частотный диапазон.

Диапазоны частот в технологии RFID

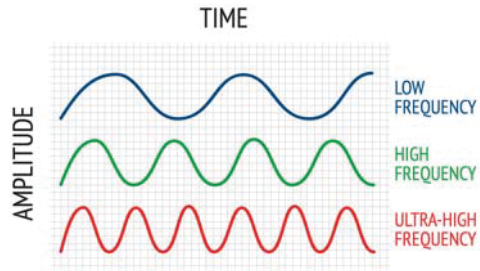


Рисунок 1.

Устройства радиочастотной идентификации (RFID) передают и принимают радиочастотное электромагнитное излучение, поэтому рабочие частоты таких устройств должны быть регламентированы таким образом, чтобы не создавалось помех службам экстренного реагирования, а также другим радиослужбам: операторам мобильной связи, ТВ и радиовещания. В каждом регионе мира (стране) изначально складывались свои специфические особенности использования радиочастот. Однако создание уникальной закрытой системы радиочастотной идентификации в каждом регионе приведёт к бессмысленному расходованию сил и средств. Все эти предпосылки привели к формированию совместимых систем и использованию стандартных диапазонов частот. Системы радиочастотной идентификации (RFID) могут работать в достаточно широком диапазоне частот от длинных до микроволн, т.е. от 125 кГц до 5,8 ГГц.

В настоящий момент широко используются следующие стандартизированные диапазоны частот:

- Низкие частоты (НЧ, LF) – 125-134 КГц
- Высокие частоты (ВЧ, HF) – 13,56 МГц
- Ультра-высокие частоты (УВЧ, UHF) – 860-960 МГц
- Микроволны (SHF) – 2,4 ГГц

Низкие частоты (НЧ, LF) – 125-134 КГц

Низкие частоты называются в иностранных источниках LF RFID (т.е. Low Frequency). Считывающее оборудование и радиометки этого типа появились раньше всего, в середине-конце 80-х годов прошлого века, однако они широко применяются и сегодня. Ключевой особенностью этого частотного диапазона RFID является то, что для него не существует общеупотребительных стандартов. Это обуславливает использование нескольких схем модуляции радиосигнала и нескольких разновидностей кодирования передаваемых данных, что в свою очередь определяется используемой в метке микросхемой транспондера.

- **Максимальное расстояние считывания:** от 3 до 70 см.
- **Скорость передачи данных радиометка-считыватель:** около 9600 бит/сек.
- **Наличие антиколлизии:** есть, но не у всех микросхем.
- **Объём памяти радиометки:** 32-1024 байта.
- **Существующие типы радиометок:** диски, цилиндры, стеклянные капсулы, RFID-гвозди, RFID-болты, корпусные метки, брелоки, БСК, браслеты, prox-карты.
- **Существующие типы считывателей:** стационарные «моноблоки», стационарные с выносной антенной, настенные, ручные считыватели, модули.
- **Рекомендации по выбору меток и оборудования:** необходимо убедиться, что в списке поддерживаемых считывателем микросхем RFID-тэгов указан совместимый формат радиометки.

Низкие частоты (LF) **125-134 КГц** по стандарту ISO 14223, ISO 11785, ISO 18000-2 применяются там, где допустимо небольшое расстояние между объектом и ридером: логистика, автоматизация производства, СКУД на основе prox-карт, RFID-брелоков, браслетов, идентификация животных.

Высокие частоты (ВЧ, HF) – 13,56 МГц

Высокие частоты в иностранных источниках обозначаются HF (High Frequency). Это рабочая частота, для которой впервые введены общемировые стандарты ISO 14443 (proximity-карты) и ISO 15693 (vicinity-карты). Все радиометки и считыватели этого стандарта поддерживают антиколлизию.

- **Максимальное расстояние считывания:** от 3 до 100 см.
- **Скорость передачи данных радиометка-считыватель:** до 64 кбит/сёк.

Высокие частоты (HF) **13,56 МГц** работают в стандартах ISO 14443, ISO 15693, ISO 10373,

ISO 18000-3. Используются там, где необходимо передавать относительно большие объёмы данных: в СКУД на основе Prox-карт, брелоков, браслетов; для идентификации товаров в складских системах и книг в библиотечных системах.

Ультра-высокие частоты (УВЧ, UHF) – 860-960 МГц

Обозначение этой полосы частот – UHF (Ultra High Frequency). Толчком к развитию этой технологии послужила разработка стандарта EPC. В силу ограничений на использование радиочастотного спектра в Европе применяется разновидность с частотой 865-868 МГц, мощностью сигнала до 0.5 Вт и переключением каналов в рамках диапазона. В США используют частоты 903-928 МГц при мощности сигнала 1 Вт. Ключевые стандарты в данной области – EPC и ISO 18000-6.

- **Максимальное расстояние считывания:** от 10 см до 70 м.
- **Скорость передачи данных радиометка-считыватель:** до 128 кбит/сёк.
- **Наличие антиколлизии:** есть до 150 меток/сёк.
- **Объём памяти радиометки:** 64-1024 бит (ISO), 64 или 96 бит (EPC).
- **Существующие типы радиометок:** корпусные метки для металлических предметов, смарт-этикетки.
- **Существующие типы считывателей:** стационарные «моноблоки», стационарные с выносной антенной, ручные считыватели.
- **Рекомендации по выбору меток и оборудования:** требуется убедиться, что считыватель и радиометка используют один и тот же стандарт. Для EPC важна поддержка такого типа меток, как EPC Class 0, 0+, 1, G2.

Сверхвысокие частоты (UHF) **860-960 МГц** в стандартах ISO 15961, ISO 15962, ISO 15963 I-CODE, ISO 18000-4, ISO 18000-6. Используются в тех проектах, где требуются повышенная дальность и высокая скорость чтения, – в системах логистики и учёта движения транспорта.

Микроволны (SHF) – 2,4 ГГц

Этот частотный диапазон – микроволновый RFID, относится к UHF. Общепринятых стандартов здесь почти не существует, в некоторых странах использование законодательно запрещено. Существующие стандарты ISO 10374 (RFID-идентификация грузовых контейнеров и железнодорожного транспорта) и ISO 18000-4 распространены достаточно мало. В большинстве случаев оборудование и радиометки – это закрытое propretiary-решение производителя, не совместимое ни с чем другим.

- **Максимальное расстояние считывания:** 2-10 м.

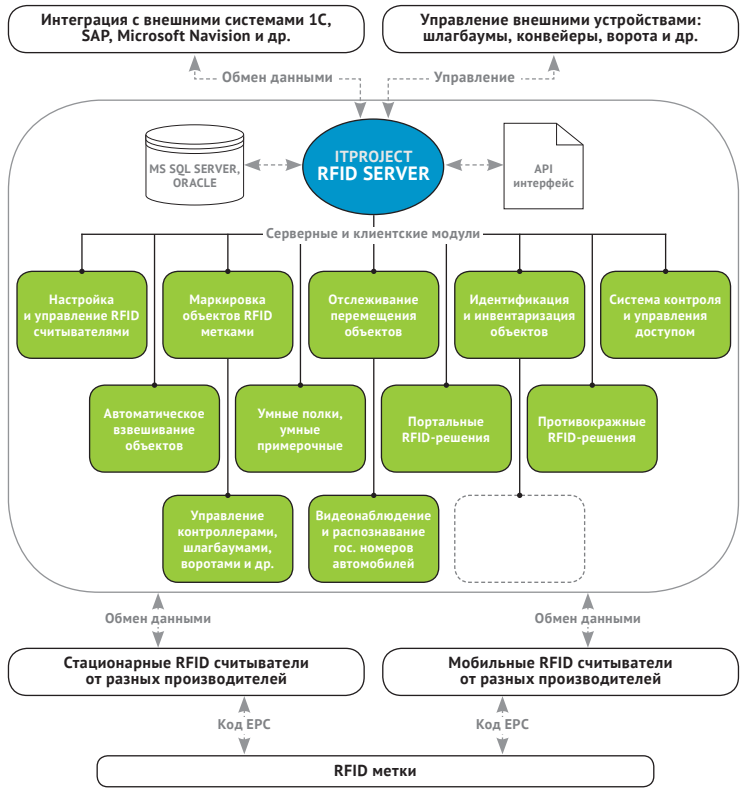


Рисунок 2. IT-платформе «ITProject RFID Platform».

- **Скорость передачи данных радиометка-считыватель:** до 128 кбит/сёк.
- **Наличие антиколлизии:** есть.
- **Объём памяти радиометки:** от 64 бит до 32 кбит.
- **Существующие типы радиометок:** корпусные метки для металлических предметов.
- **Существующие типы считывателей:** стационарные «моноблоки», стационарные с выносной антенной, ручные считыватели.

Наконец, пробравшись сквозь дебри определений и физических свойств радиоволн, можно перейти к увлекательному повествованию о непосредственной деятельности нашей компании.

Наша компания, пройдя достаточно большой путь и изучив все возможности использования радиочастотных волн как в теории, так и на практике, вобрав всё лучшее и отбросив всё лишнее, готова делиться полученными знаниями с нашими клиентами и обеспечить основу для успешного развития их бизнеса за счёт внедрения RFID-технологи и, что позволит значительно повысить эффективность бизнес-процессов на предприятии.

Портфель решений компании включает RFID-системы контроля доступа и мониторинга перемещений людей и транспорта, кон-

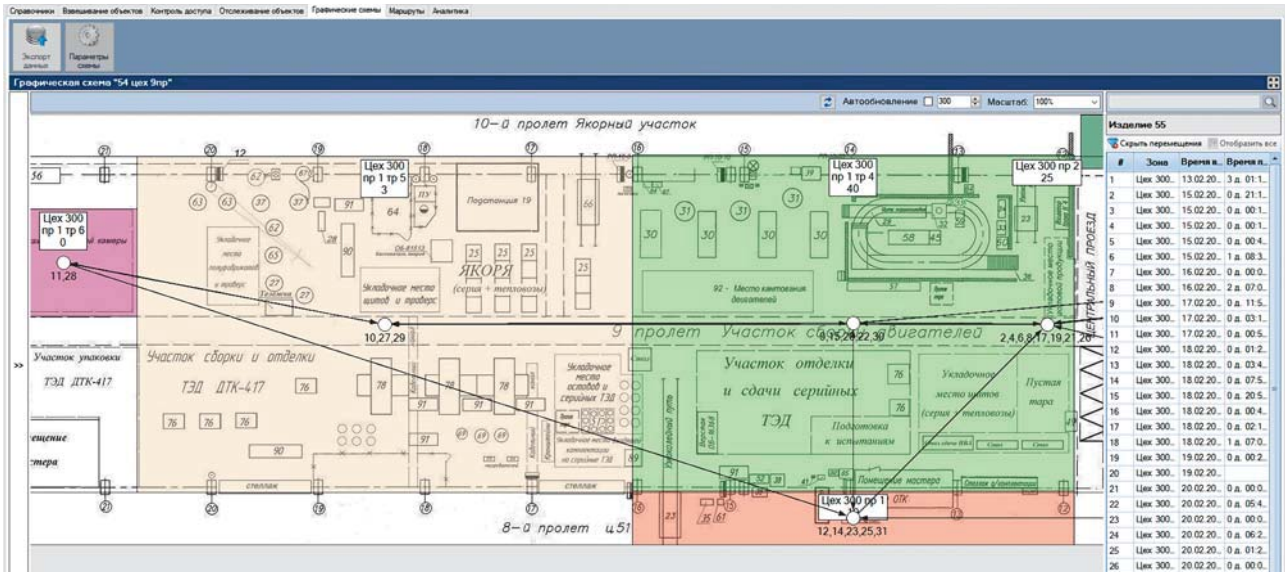


Рисунок 3. «ITProject RFID Tracking System».

троля рабочего времени и производственных процессов, отслеживания перемещения товаров и основных средств, управления автоматическими системами обеспечения безопасности, управления процессом производства. Решения компании «АйТи-Проект» используются в промышленном производстве, в торговле, транспортными и логистическими компаниями, коммерческими и государственными структурами, организаторами крупных мероприятий с большим количеством посетителей.

Все отраслевые решения построены на базе, разработанной нами ИТ-платформе ITProject RFID Platform (рис. 2).

Программно-аппаратная платформа ITProject RFID Platform состоит из движка и дополнительных клиентских и мобильных решений, которые обеспечивают простую разработку и развёртывание RFID-систем различной степени сложности. Использование ITProject RFID Platform позволит сразу приступить к внедрению любой RFID-системы на предприятии и получить желаемые результаты в короткие сроки с небольшими затратами в сравнении с ценой собственной разработки. ITProject RFID Platform легко масштабируется, т.е. сегодня можно внедрить одно RFID-решение, а завтра – другое. Очень важно, что для этого не потребуется использование нового программного обеспечения для решения других задач.

Отраслевые решения на базе ITProject RFID Platform

Перемещение объектов:

• На производстве

Промышленная автоматизация – это комплекс программно-аппаратных решений, применение которых позволяет человеку контролировать производственный процесс, не участвуя в нём непосредственно.

На современных предприятиях автоматизация производства на базе RFID-технологии осуществляется с целью сократить численность персонала, который занят обслуживанием производственного оборудования, увеличить производительность, улучшить условия труда и сделать производство более безопасным.

Повышение эффективности производственной деятельности достигается за счёт точного контроля над всеми этапами производственного процесса, что является основой в процессе построения автоматизации управления предприятием.

Автоматизация производства на базе RFID-технологии позволяет решить задачу оптимальной загрузки оборудования и персонала, снизить себестоимость продукции

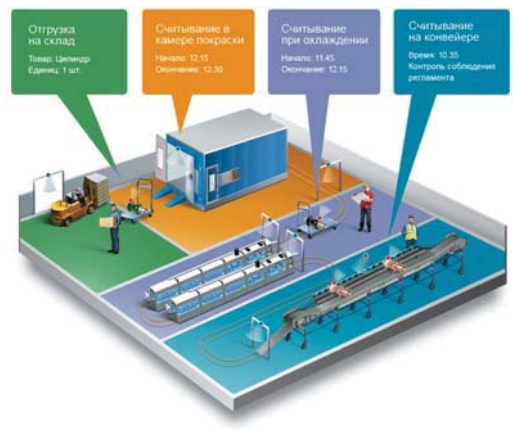


Рисунок 4.

без потери качества и оптимизировать процессы на производстве.

Иными словами, это повышает конкурентоспособность предприятия посредством снижения себестоимости производимой продукции, благодаря сокращению временных и финансовых издержек, вызванному снижением роли человеческого фактора.

Используя клиентский модуль ITProject RFID Tracking System, система может:

- регистрировать события, такие, как время входа, выхода, нахождения объекта в конкретной зоне, например соблюдение времени нахождения мясных продуктов в камере копчения или камере охлаждения;
- быстрая реакция на заданные в системе события, например в случае невыполнения определённых условий можно отсылать оповещение или начинать вести видеонаблюдение;
- фиксирование состояния продукции: всегда можно автоматически узнать, на каком этапе находится продукт и с точностью отследить его состояние. Это облегчает последующий контроль качества и сбор полезной статистики;
- наблюдение за маршрутом движения деталей: список деталей любого механизма в конкретной зоне считывания можно показать в графическом или табличном виде;
- анализ дополнительных сведений: на каждом этапе портативный считыватель может записать на метку или в базу данных актуальную информацию об объекте, например точные данные о температуре обработки или времени нахождения;
- быстрое отслеживание объектов: система позволяет быстро находить любой объект, что особенно актуально для крупных предприятий;
- индивидуализация производства: благодаря RFID-меткам, расположенным на деталях механизма, можно использовать индивидуальные параметры, например определённый цвет кузова или материал обивки салона в автомобиле, это позволит чётко собирать любые механизмы с разной комплектацией..

• Для аэропортов

В каждом аэропорту есть стойка с надписью Lost&Found для обращений пассажиров, чей багаж потерялся при перелёте. Особенно часто это происходит при транзитных рейсах. Люди борются с потерями самостоятельно: покупают яркие чемоданы, привязывают к ручкам сумок бирки со своим телефоном и ФИО, но грузчики на них не реагируют. Это происходит в аэропортах всего мира.

Рисунок 5.

Затраты на компенсацию утерянного багажа снижают прибыль авиакомпаний. Убытки от испорченной репутации посчитать труднее: они могут намного превышать прямые расходы.

Основным источником ошибок в системе сортировки и загрузки багажа на борт самолёта является человек. Невнимательность, беспечность, усталость, даже плохие погодные условия повышают количество ошибок персонала. Решением проблемы становятся автоматизированные системы сортировки и отслеживания багажа, в которых участие человека сведено до минимума.

Мы можем:

• Отслеживать местонахождение багажа.

Багаж с RFID-меткой всегда под контролем. Оператор системы в любой момент легко определит, где он находится: в самолёте, на погрузке, конвейере или где-либо ещё.

• Упростить отчётность и ускорить документооборот.

В базе данных хранится информация о маршруте и текущем местонахождении каждой багажной единицы. Ведомости отправленного багажа для экипажа самолёта формируются на лету и распечатываются за секунды.

• Сохранить багаж.

Багаж с меткой не может бесследно пропасть: система покажет, где он был в последний раз. Это дополнительный плюс к защите личных вещей клиентов.

• Сократить число задержек рейсов.

Применение RFID-системы втрое сокращает время сортировки и погрузки багажа в самолёт, что в свою очередь поможет аэропорту следовать чёткому расписанию. Теперь время на подготовку контейнерной ведомости и багажного манифеста составляет 50 секунд вместо 3 минут. Время комплектации багажа – 1 минута на единицу багажа вместо 2.9 минут. Время снятия багажа с рейса – 2-3 минуты вместо 10-20 минут.

• Сократить эксплуатационные расходы.

За счёт более эффективного использования рабочего времени персонала и сокращения времени ожидания транзитных пассажиров.

• Уменьшить ошибки по причине человеческого фактора.

При старой системе при погрузке или выгрузке багажа грузчики могут перепутать номера или метки. С RFID-системой такого не случится: система не ошибается, в отличие от человека, она не устаёт и всегда работает со стопроцентной эффективностью, поэтому путаница с выдачей исключена.

• Повысить производительность работы грузчиков в аэропорту.

Багажный участок сможет обрабатывать в 3-7 раз больше багажа (причём, без ошибок) существующим составом. Без RFID-системы в среднем грузчик выполняет до 4300 наклонов за смену, из которых только 645 (15%) действительно полезны.

• Для животноводства

Представьте, что вы на ферме, где содержится тысяча коров (или лошадей, или коз – любого домашнего скота). Большинство здоровы, но несколько только что отелились и требуют особенного ухода и кормления. И они все должны вовремя получать еду, воду и пастись на свежем воздухе. Если вовремя на заметить перемен в поведении животного, оно может просто погибнуть.

Как отследить перемещение каждого животного, регулировать его кормление и здоровье? Используя простые бирки или клейма, вы сможете идентифицировать животное, но всю информацию по его кормлению придётся хранить в другом месте – на бумаге или в базе. Но для того, чтобы соотнести её с животным, требуется много времени и сил, а значит, ошибки неизбежны.

Не самый лёгкий и очевидный, но точно самый надёжный путь решения проблемы с отслеживанием и контролем за животными – автоматизировать большинство процессов с использованием RFID-технологии. Что тогда заменит пластиковые бирки и бумажные записи?

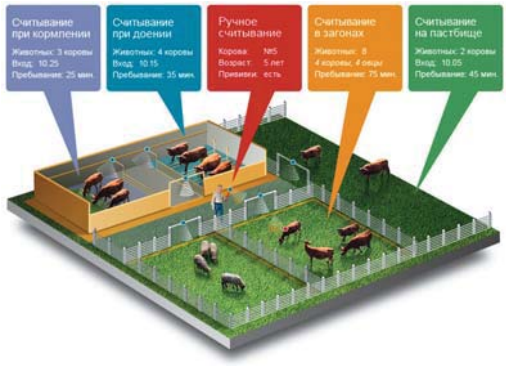


Рисунок 6.

Мы разработали RFID-систему, основанную на чипировании животных, крупного рогатого скота (КРС) и птиц. Система позволит вам полностью контролировать все процессы, связанные с перемещением, уходом и питанием животных.

RFID-система включает в себя особые метки, оборудование и программное обеспечение.

Антенны меток посылают радиоволновой сигнал, который можно уловить специальным считывателем (ручным или стационарным). Вся полученная информация поступает на компьютер.

Метки бывают нескольких видов: для чипирования крупных животных, крупного рогатого скота (КРС) чаще всего используются пластиковые бирки, цепляющиеся на уши, для чипирования птиц – небольшие колечки на лапы.

Быстрая идентификация на расстоянии 1-5 метров.

Все данные о животном можно за пару секунд считать с достаточно большого расстояния – до пяти метров, поэтому человек со считывателем может стоять даже за ограждением загона.

Безопасность животных. Вы легко можете узнать, если какая-то корова (или лошадь, или овца) вдруг оказалась не в своём загоне или не пришла с пастбища, и вернуть её. А также вовремя диагностировать болезни и реагировать на них.

Электронный паспорт. Для каждого животного можно завести свой электронный документ принятого мирового стандарта, в котором будет собрана вся необходимая информация: порода, прививки, вязки и т.д.

Упрощается кормление. Установив считыватель около кормушек, можно легко определить и изменить информацию о специфике и количестве корма для каждого животного, а также сопоставить эти сведения с получаемыми надоями.

• Решение для транспорта и логистики

Везде, где есть необходимость отслеживать перемещение транспорта, контролировать его доступ на объект или оценивать эффективность использования транспортных средств, остро стоит проблема человеческого фактора. Он становится одной из главных проблем в процессе автоматизации, поскольку приводит к ошибкам, задержкам и сбоям, а значит, к убыткам.

Рисунок 7. «ITProject RFID AccessSystem»

Эта проблема актуальна для многих предприятий, складов, грузовых терминалов, государственных учреждений, транспортных компаний и даже для платных автодорог (поскольку основной задачей для них является эффективное управление транспортом и грузопотоками).

Система для контроля доступа и отслеживания перемещения людей/транспорта/объектов, контроля вноса или выноса имущества, используя клиентский модуль ITProject RFID AccessSystem, работает в составе программно-аппаратной платформы ITProject RFID Platform и предназначена для автоматизации задач контроля въезда/выезда транспорта на территорию, контроля вноса/выноса имущества, контроля доступа людей, а также задач автоматического контроля за перемещением объектов с использованием технологии радиочастотной идентификации (RFID).

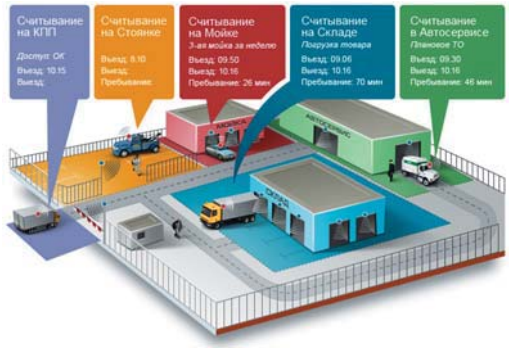


Рисунок 8.

Отличительной особенностью данного решения является удалённое считывание (0,5-7 метров) RFID-метки с человека, автомобиля или другого объекта. Для доступа на объект нет необходимости показывать пропуск или прикладывать его к считывателям, или выходить из машины, открывать стекло автомобиля и тянуть руку к считывателю. В случае предоставления доступа происходит автоматическое открытие турникета или поднятие шлагбаума для проезда автомобиля.

Можно создавать различные схемы доступа на объект, например одна группа сотрудников будет иметь доступ на производственную площадку и на склад, а другая – доступ в лабораторию. Изменить схему доступа можно в любой момент, что позволит быстро отреагировать на непредвиденную ситуацию.

Модуль ITProject RFID Access System может работать как в составе систем СКУД существующих пропускных пунктов, так и самостоятельно, предоставляя ограниченный доступ в требуемую зону, регистрируя объект и время его пребывания на территории охраняемого объекта. В случае необходимости можно посмотреть историю перемещения человека или автомобиля по территории охраняемого объекта.

• Система для Retail

Самая губительная черта для владельцев розничной сети – невнимательность. Необходимо контролировать огромные товаропотоки и постоянно проводить инвентаризацию. Из-за ошибок, недосмотра и недостаточного контроля возникают потери, которые только на первый взгляд кажутся мелкими. На деле, недостачи и кражи могут составлять до 50%

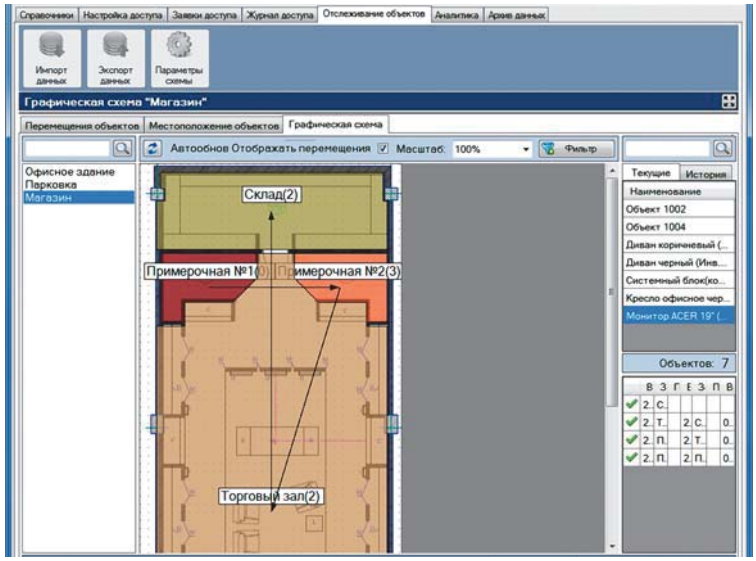


Рисунок 9. «ITProject RFID Retail System»

Рисунок 10.

убытков! Как следить за всеми процессами и сохранять прибыли?

Можно пытаться организовать работу, используя штрихкоды, но это влечёт за собой огромные трудозатраты и неизбежные ошибки. Чтобы предотвратить дальнейшие потери, надо подойти к вопросу комплексно. И один из самых важных аспектов этого подхода – непрерывный надёжный контроль. Но как его обеспечить? Как защитить себя от краж и потерь товаров во время инвентаризации, а также избавиться от лишних трудозатрат?

Решение есть: мы создали систему для сбора статистики о востребованности товаров, отслеживания местоположения и мониторинга перемещений товаров, персонала и покупателей в магазине.

Клиентский модуль ITProject RFID Retail System работает в составе программно-аппаратной платформы ITProject RFID Platform и предназначен для автоматизации учётных операций, формирования отчётов, сбора статистики о востребованности товаров, защиты от краж, мониторинга перемещений товаров, персонала и клиентов в магазине в режиме ON-LINE. Данный модуль предназначен для клиентов, которые хотят получать дополнительную аналитику с возможностью её отправки в системы типа 1С, SAP, Microsoft Navision и др. Используя данное решение, можно в кратчайшие сроки интегрировать RFID-оборудование в инфраструктуру предприятия.

Всё, что описано выше, – только часть из разработанных и внедрённых нами решений.

Каждый наш проект – это большая командная работа, где каждый решает определённый круг задач.

Наши преимущества при реализации RFID-проектов:

- Отличительной особенностью компании «АйТиПроект» при реализации RFID-проектов является ставка на инновационность, качество и надёжность. Наши специалисты имеют большой опыт внедрения RFID-технологии на предприятиях, поэтому наши заказчики вне зависимости от отрасли, как правило, получают современные RFID-решения, порой не имеющих аналогов в Мире.
- Основным принципом, являющимся залогом успешной работы, мы считаем постоянное взаимодействие с заказчиком. Это позволяет оперативно реагировать и адаптировать наши RFID-решения к мельчайшим нуждам пользователей, что существенно сокращает процедуру последующих внедрений.
- На сегодняшний день наша компания – это не просто флагман в области RFID-решений, а уже платформа IOT, и ближайший план на будущее – развитие и освоение новых технологий и ИТ-возможностей.

---

aimu проект

разработчик RFID-систем

Компания «АйТиПроект» *– это RFID-интегратор и разработчик программного обеспечения для RFID-систем. Компания имеет большой опыт в области разработки RFID-систем и успешно внедряет готовые отраслевые RFID системы на предприятиях.*

www.itproject.ru

«Headtechnology»

Уважаемые читатели! Хотела бы начать свою статью со слов благодарности коллегам из редакции журнала CIS за предоставленные возможности участвовать в конкурсе «Мисс CIS», рассказать о компании, в которой я сейчас тружусь, и о своей роли в ней!

Елена Титович
Компания «Headtechnology»

Итак, представлюсь, меня зовут Елена Титович, я региональный директор по продажам компании Headtechnology, работаю в ИТ-сфере более 15 лет, занимаюсь направлением информационной безопасности почти 10 лет. Headtechnology представляет собой группу компаний, имеющих 8 офисов, территориально расположенных в Восточной Европе, странах Балтии, России, странах СНГ, Центральной Азии и Турции. Мы являемся международной компанией, работающей более чем в 35 странах. Я отвечаю за развитие бизнеса в таких странах, как Россия, Беларусь, Казахстан, Кыргызстан, Узбекистан и Турция.

Ключевое направление компании Headtechnology – дистрибьюция решений по информационной безопасности и защите данных, работа и развитие долгосрочных успешных отношений с локальными системными интеграторами, партнёрами и перселерами. В портфолио компании тщательно отбираются самые актуальные и важные системы (в основном, программное обеспечение), которые уже активно востребованы и используются в Западной Европе и Америке, необходимы корпоративным компаниям, среднему и крупному бизнесу, государственному сектору в регионах нашего присутствия. Мы также работаем с заказчиками, чтобы оперативно доносить передовой опыт и технологии, предоставляем профессиональную техническую поддержку на этапах пресейла, внедрения и дальнейшего сопровождения систем.

Несколько слов о ключевых вендорах, дистрибьюцией которых мы занимаемся.

MobileIron – UEM платформа для защиты и управления мобильными устройствами, приложениями и контентом. Более 5 лет находится в лидерах Gartner в части MDM | EMM | UEM решений. Сотни тысяч инсталляций приложения в глобальных международных компаниях, десятки крупных довольных заказчиков в России.

Forescout – платформа сетевой безопасности, система NAC+ для мониторинга, контроля и управления всеми IP устройствами, классификация всех устройств, предотвращение возможных угроз со стороны IOT. Удобная система для создания политик ИБ с целью налаживания взаимосвязей между всеми подсистемами информационной безопасности – UEM, IDM, PIM | PAM, SIEM и другими. Лидер Gartner с успешными реализациями решения в финансовом секторе, нефтегазовой отрасли, телеком операторах, ритейле и других компаниях.

Accellion – защищённое корпоративное облако внутри компании для безопасного обмена данными как внутри неё, так и с внешними контрагентами. Практически как корпоративный dropbox для удобной совместной работы с документами, создание «секретных комнат», обмен файлами без ограничения размера, функции автоматизации, интеграции с DLP, CRM, ERP системами, GDPR отчётность. Эту систему активно используют Банковский сектор, страховые и медицинские компании, ритейл и промышленные организации.

Миссия компании – сделать мир безопаснее! Наша команда искренне верит в то, что предоставляя современные инструменты и технологии компаниям среднего и крупного бизнеса, мы делаем мир и жизнь каждого индивидуума безопаснее в части работы с киберпреступниками и злоумышленниками.

headtechnology
it-security distribution

*Основное направление деятельности **компании «Headtechnology»** – дистрибьюция решений по информационной безопасности.*

headtechnology.com

Издательство «Эксмо»

Ирина Василевская
Издательство «Эксмо»

Я работаю в издательстве «Эксмо» – издательство № 1 в России – в нём трудятся тысячи сотрудников.

«Эксмо» является одним из лидеров книжного рынка Европы по тиражам выпускаемой художественной, развлекательной, прикладной и детской литературы, согласно данным Российской книжной палаты.

Компания основана в 1991 году. Уже к середине 1990-х издательство заняло лидирующие позиции на российском книжном рынке. Интеграция с ведущими участниками книжного рынка стала закономерным шагом в развитии бизнес-потенциала издательства. В 2012 году к «Эксмо» присоединилось издательство «АСТ», в 2014 – «Дрофа», в 2015 – «Вентана-Граф». В 2017 году объединённая издательская группа «Дрофа-Вентана» была преобразована в Корпорацию «Российский учебник».

Каждый год издательство «Эксмо» выпускает порядка 80 миллионов книг. Издательство «Эксмо» входит в Российский книжный союз, принимает активное участие в мероприятиях, направленных на поддержку интереса к чтению у россиян, развитие диалога с профильными ведомствами, общественными организациями и представителями бизнес-сообщества с целью развития книжной отрасли.

Среди наиболее известных социальных проектов издательства есть такие: кампания с участием медиа-персон «Читай книги – будь личностью!», кампании «Читайте детям книги», «Хочу познакомиться с умным!» и др. Издательство «Эксмо» ежегодно принимает участие в ключевых событиях книжной отрасли России, среди которых Книжный фестиваль «Красная площадь», Московская международная книжная выставка-ярмарка на ВДНХ, Санкт-Петербургский книжный салон и др. В числе проектов издательства по популяризации чтения планируется открытие виртуальных библиотек в аэропортах Шереметьево и Пулково.

Моя история в «Эксмо» началась в 2004 году. На тот момент я училась в Московском государственном университете культуры по специализации «Реклама» и искала работу. Волею судьбы я оказалась в динамично развивающейся книжной компании. Мне предложили участие в интересном проекте по внедрению масштабной ERP-системы в качестве специалиста нормативно-справочной информации (НСИ), и несмотря на другую профессиональную область, я решила попробовать себя в сфере информационных технологий (ИТ).

Университет я окончила с отличием, и вот уже более 15 лет продолжаю трудиться в сфере ИТ издательства «Эксмо». За это время я успела вырасти до руководителя группы, окончить многочисленные тренинги и курсы, принять участие в различных масштабных проектах и быстро освоиться в издательском деле.

НСИ в издательстве «Эксмо» – это центр единого информационного пространства, включающий в себя справочники, классификаторы, стандарты, идентификаторы и регламенты. Ведение нормативно-справочной информации – ответственное дело, требующее внимания, аккуратности, оперативности и высокого профессионализма.

Ввод, изменение, удаление, корректировка, выгрузка, загрузка, – одним словом, порядок в справочниках – главная заслуга моей группы. Методическая поддержка пользователей, консультирование, а также документирование, учёт, ведение и актуализация НСИ – важные аспекты в нашей ежедневной работе. Плоды и результаты моей работы, моя гордость – актуальные и идеальные справочники системы.

Работа в «Эксмо» стала неотъемлемой частью моей жизни. Издательство «Эксмо» – флагман российского книгоиздания, большая дружная команда и мой второй надёжный дом.

ЭКСМО

Издательство «Эксмо» *– универсальное издательство № 1 в России, является одним из лидеров книжного рынка Европы.*

www.eksmo.ru

Издательство «Эксмо-АСТ» и «Росучебник»

Издательство «Эксмо» было основано как дистрибутор книжной продукции, а позже начало самостоятельную издательскую деятельность. Уже к середине 90-х годов «Эксмо» достигло лидирующих позиций на российском книжном рынке.

Каждый год «Эксмо» выпускает порядка 80 млн книг, что составляет примерно 40% книг в России. Среди авторов – Дарья Донцова, Александра Маринина, Татьяна Устинова, Павел Астахов, Олег Рой, Вадим Панов, а также солист группы Rammstein – Тилль Линдеманн.

«АСТ» – второе по величине издательство, которое более 25 лет выпускает прикладные издания, интеллектуальную и развлекательную литературу, русскую и зарубежную классику. В год издаёт более 40 млн книг. Знаменитые авторы «АСТ» – Сергей Лукьяненко, Дмитрий Глуховский, Борис Акунин, Людмила Улицкая и другие.

В 2014 году произошло слияние этих двух книжных издательств, титанов в своей области – «Эксмо» и «АСТ». А позже мы «взяли под крыло» издательства «Дрофа» и «Вентана-Граф» (переименованные в «Росучебник»). Теперь наша дружная команда называется Группа компаний «Эксмо-АСТ» и Корпорация «Российский учебник».

Являясь крупнейшим объединением ведущих российских издательств, мы осознаём долю своей ответственности за развитие книжного рынка. Поэтому для нас важно каждый день выступать создателем и двигателем инициатив по совершенствованию отрасли на федеральном уровне, оправдывая свои лидерские позиции.

Для поддержания своего высокого статуса, помимо творческого подхода художников и редакторов, технологов и верстальщиков, необходимы профессиональные знания и опыт сотрудников технической поддержки.

ИТ-специалисты как по мановению волшебной палочки могут сотворить сказку: устранить сбой в работе принтера-обжоры, который стал «жевать» бумагу; «оживить» систему, спасая от ошибки BSOD; решить вопрос с «непослушной» мышкой, когда курсор стал «дрожать», возможно, от страха; помочь с настройкой вебинара; закупить «сильный» ноутбук для аналитических задач и «подружить» различные виды техники друг с другом. Всем этим и многим другим занимается наш ИТ-отдел.

Заявки от пользователей поступают операторам 1-ой линии техподдержки. Здесь происходит обработка, сортировка и распределение задач на 2-ю и 3-ю линии. Я являюсь руководителем 1-ой линии и слежу за обеспечением высокого уровня работы операторов, общаюсь со «сложными» пользователями, а также администрирую базу ServiceDesk. А ещё с удовольствием воплощаю в жизнь свои идеи в сфере ИТ.

Примерно 2,5 года назад у меня возникло желание провести ликбез среди пользователей по работе с ИТ-ресурсами. Мы создали кнопку с названием «ИТ-хэлп» на рабочих столах офисных ПК, при клике на которую любой сотрудник в режиме 24/7 может получить доступ к инструкциям по ИТ-сервисам. Предполагалось, что кнопку «ИТ-хэлп» будут использовать рядовые сотрудники. Но ею заинтересовались руководители высшего звена, которые теперь активно применяют её в своей работе. Это был колоссальный успех!

Позже мы улучшили интерфейс и работу поиска по кнопке «ИТ-хэлп», синхронизировали её с базой ServiceDesk, что помогло вдвое сэкономить время пользователей на регистрацию заявок. А также мы повысили уровень их компьютерной грамотности.

Мы и сейчас продолжаем улучшать качество ИТ-сервисов, ставя перед собой новые интересные задачи.

Евгения Цуркан
ГК «Эксмо-АСТ» и «Российский учебник»

«Российский учебник» *– российское специализированное издательство учебной литературы. Выпускает учебную и методическую литературу для начальной, основной и средней (в том числе национальной) школы; пособия для дошкольных организаций; картографическую продукцию*

www.rosuchebnik.ru

«Центр Информационных Технологий»

Ануш Хоменко
ЧУ ОДО «Центр Информационных Технологий»

Меня зовут Ануш, и с 2011 года я начала свой старт в сфере ИТ. Увлекаться сферой информационных технологий, в частности графическим дизайном и web-разработкой, я начала со средней школы. После уроков я мчалась на компьютерные курсы, где проводила многие часы. Потом увлечение переросло в профессиональную деятельность, чему я бесконечно рада! Ведь я отношусь к той категории людей, которые занимаются любимым делом.

Свой профессиональный опыт я нарабатывала в разных областях и ипостасях: работа в офисах ИТ-компаний, дизайн студиях/бюро, фриланс. Всё это позволило быть той, кем я сейчас являюсь. А в данный период жизни я посвятила себя Центру Информационных Технологий и Высшей Школе Программирования, которая создана на его базе. Мои рабочие будни насыщены и разнообразны. Мы занимаемся разработкой ПО, создаём сайты для наших заказчиков из разных отраслей, имеем свой сервисный центр и, конечно же, дизайн-студию. Но всё это вторично, сейчас мы сконцентрированы на нашей Школе, в которой сами и преподаём: обучаем тому, что умеем. Делиться опытом, знаниями, умениями – это мегакруто! Изо дня в день видеть, как многого достигают твои ученики – это не может оставить безучастным.

Работа – это моя отдушина. Наш коллектив молод, крут и постоянно растёт. Мир вокруг меняется с каждым днём, и меняется в лучшую сторону, благодаря, в том числе, и нам. Мы не только оптимизируем бизнес-процессы наших заказчиков, обеспечиваем мегакрутыми лендингами, интернет-магазинами и т.д., но и взращиваем новое поколение себе на смену. Наши ученики – это перспективные ИТ-специалисты в разных областях, количество отделений в Школе радует разнообразием. Но ещё больше радует то, что, являясь практикующими преподавателями, мы даём нашим ученикам концентрированную учебную программу, которая в итоге делает их прекрасными специалистами! Я считаю, что моя работа очень важна, так как занимаюсь развитием и популяризацией ИТ на уровне города и региона. Важно то, что мы доносим до подрастающего поколения, что стране нужны ИТ-специалисты, ей очень не хватает квалифицированных кадров. Также мы сами проводим ИТ-мероприятия и участвуем в таковых, и это тоже значимо.

Работать в ИТ – это мечта, и здесь нет деления профессий на мужские или женские. Специализации настолько разнообразны, что каждый может найти своё место. Главное – это любить то, что ты делаешь!

ВЫСШАЯ ШКОЛА ПРОГРАММИРОВАНИЯ

ЧУ ОДО «Центр Информационных Технологий» *– Высшая Школа Программирования*

www.it-proger.com

«Arkell»

LIMA – новый сотрудник любого отдела маркетинга

Пора забывать о постапокалиптических сюжетах восстания машин и учиться использовать во благо то, что создал человеческий интеллект. Кажется, что машины порабощают человека, но нет. Только Человек имеет потенциал, талант и время, а технологии лишь помогают грамотно распорядиться его ресурсами. Это человек оказывает услуги для бизнеса, а бизнес работает только для человека, технологии лишь выступают инструментом для выстраивания алгоритмов и соединения этих двух невероятно мощных сил. Именно это и стало основой для ИТ-стартапа LIMA.

До сих пор без внедрения технологий остаются тысячи профессий – это оправдано, когда задача требует творческого мышления и человеческого интеллекта. Но мы сторонники такой идеи, где российский бизнес адаптирован к мировым тенденциям и современному темпу, – это значит, что должно быть оцифровано всё, что имеет заранее известный алгоритм действий.

Мы создали концепцию мобильного приложения, которое внесёт существенные изменения в нишу найма временных сотрудников – это рынок BTL и Event. Потребители таких услуг – компании ритейл-рынка, растущего и исчисляемого десятками миллионов долларов. Чтобы избавить ритейлеров от боли поиска временного персонала для проведения промоакций и работы на выставках, компания Arkell IT-Solution решила создать уберизированный сервис для решения этой задачи.

Концепция LIMA

LIMA – это платформа для бизнеса, сервис для поиска и найма временных сотрудников для проведения промоакций, работы на мероприятиях любого масштаба. LIMA выступает альтернативой существующим BTL-агентствам – это принципиально новая технология для бизнеса.

Разработанная механика приложения такова: заказчиком выступает юридическое лицо. Он размещает заказ в личном кабинете в приложении, прописываются детали и подробности работы с описанием задач и ожидаемого результата. Программа подбирает промоутеров с желаемыми параметрами. Там же заказчик отправляет в типографию макеты для печати листовок, получает подтверждение выхода промоутера, производит оплату, скачивает закрывающие документы. Надо отметить, что такой алгоритм не подразумевает действенного участия организатора промоакции, – приложение оповещает обо всех изменениях в процессе.

Разработчики разложили на молекулы практически всю процедуру проведения промоакции от идеи и до закрытия документов. *Мы научили наше приложение видеть промоутера в реальном времени и считывать его передвижение по геолокации в заданном периметре во время исполнения заказа, делать фотоотчеты в течение работы, напоминать о начале и конце выполнения заказа и многим другим функциям. Мы создали жёсткие рамки контроля качества работы, и это было бы невозможно без внедрения технологий оцифровки бизнес-процессов.*

Внедрение любой технологии требует взрывного PR-продвижения, особенно это касается ИП-стартапов. Специалисту по PR приходится пробиваться через предубеждения, так как находится мало желающих полностью доверить свои бизнес-процессы технологиям. Здесь на помощь приходит работа в тандеме с разработчиками и изучение ИТ-технологий.

Татьяна Греханова
ИТ-студия Аркелл

LIMA

ИТ-студия Аркелл *была основана в 2014 году как студия для реализации различных веб решений. Аркелл совмещает профессиональный подход к дизайну и программированию. Компания занимается разработкой различных ИТ решений. От мобильных приложений и сайтов до сложных комплексных решений которые включают целую цепь взаимодействующих между собой «клиентов» и серверов.*

www.arkell.ru

«Axoft»

Анна Иванова
Компания «Axoft»

Axoft – № 1 в рейтинге CRN/RE «Лучшие ИТ-дистрибуторы ПО».

Axoft – сервисный ИТ-дистрибутор, работающий на рынке России и ВЕЦА. С 2004 года компания помогает ИТ-производителям, системным интеграторам, реселлерам и сервис-провайдерам обеспечивать корпоративных пользователей ИТ-решениями и сервисами, которые наилучшим образом решают их бизнес-задачи.

В портфеле Axoft представлены SaaS- и IaaS-решения, системы для обеспечения информационной безопасности, инфраструктурное, офисное и научное ПО, а также сопутствующие партнёрские сервисы: обучение, консалтинг, маркетинговая, финансовая и техническая поддержки.

По итогам 2017 финансового года оборот компании вырос на 55% и достиг 10,8 млрд рублей. Компания представлена в 28 городах 9 стран мира: России, Беларуси, Грузии, Армении, Азербайджане, Казахстане, Узбекистане, Таджикистане, Кыргызстане, Монголии.

Преимущества работы с Axoft уже оценили около 6000 компаний-участников ИТ-рынка: реселлеры программного обеспечения и системные интеграторы, разработчики программных решений, интернет-магазины и консалтинговые компании.

Мы являемся официальным дистрибутором более чем 1000 мировых производителей программного и программно-аппаратного обеспечения: Microsoft (CSP), «Лаборатории Касперского», Positive Technologies, Micro Focus (ранее Hewlett Packard Enterprise), «Кода Безопасности», Red Hat, Palo Alto Networks, FireEye, Kerio и многих других. Представленные в портфеле ИТ-решения и сервисы разнообразны с точки зрения стоимости и функционала, отвечают потребностям крупного, среднего и малого бизнеса и государственных структур.

С 2009 года Axoft входит в ТОП-5 лучших ИТ-дистрибуторов ПО, по версии CRN/RE и Astera.

В 2017 году компания заняла первую строчку рейтинга CRN/RE. Axoft ежегодно подтверждает соответствие системы менеджмента качества требованиям международного стандарта ISO 9001:2015.

В компании Axoft я работаю на должности менеджера по продажам.

Основные задачи:

- Развитие отношений с закреплёнными партнёрами:
  - установление контакта с ключевыми сотрудниками партнёра, построение с ними дружественных, партнёрских коммуникаций, повышение лояльности;
  - изучение бизнеса партнёра, определение эффективных точек соприкосновения для совместного увеличения продаж;
  - выявление, стимулирование и формирование потребностей (генерация новых интересов);
  - встречи, презентации, переговоры (в т.ч. с заказчиками партнёра);
  - консультирование партнёров по вопросам, связанным с текущей деятельностью.
- Выполнение установленных планов продаж:
  - планирование работы с партнёрами (операционное и бизнес-планирование);
  - увеличение объёмов закупок у Axoft, расширение вендорской корзины у партнёра;
  - контроль дебиторской задолженности;
  - поддержание в актуальном состоянии CRM-базы по истории взаимодействия с партнёрами (новые контакты, возможные сделки, пилоты, встречи и т.п.);
  - непосредственное достижение квартальных и годовых финансовых целей.
- Непрерывная работа над собственной экспертизой по ключевым для компании продуктам / решениям / услугам.

AXOFT

Компания «Axoft» *– сервисный IT-дистрибутор, работающий на рынке России и ВЕЦА.*

www.axoft.ru

«Positive Technologies»

Меня зовут Таня, и я работаю в самой позитивной компании, призванной сделать мир чуточку безопаснее.

Татьяна Зверева
Компания Positive Technologies

Positive Technologies более 17 лет аккумулирует экспертные знания по практической безопасности и является одним из мировых лидеров в области комплексной защиты крупных информационных систем от современных киберугроз. Компания имеет представительства и R&D-центры не только в России, но и по всему миру, в том числе в Великобритании и Чехии.

В нашей команде более 250 экспертов по защите ERP, SCADA, банков и телекомов, веб- и мобильных приложений. Более 1000 компаний используют решения Positive Technologies для анализа защищённости и соответствия стандартам, а также для мониторинга событий безопасности, блокирования атак, предотвращения вторжений, расследования инцидентов, анализа исходного кода и построения безопасной разработки.

Компания трижды становилась «визионером» в исследовании Gartner Magic Quadrant по системам защиты веб-приложений (WAF). Результаты исследований экспертов Positive Technologies используются для обновления базы знаний системы MaxPatrol, а также для разработки новых продуктов комплексной защиты: PT Application Firewall, PT Application Inspector, MaxPatrol SIEM, PT ISIM, PT MultiScanner и других. Эти решения позволяют обеспечить безопасность веб-приложений, оценить уровень защищённости сетей, блокировать атаки в режиме реального времени, контролировать выполнение нормативных требований и соответствие государственным и корпоративным стандартам, а также обучать специалистов по безопасности.

Кроме того, Positive Technologies является организатором ежегодного международного форума Positive Hack Days, развивает портал www.SecurityLab.ru.

В этой успешной профессиональной команде я занимаюсь продвижением продуктов и услуг, потому что мне близки идеология и миссия компании. У нас и правда классная команда, с которой мы делаем мир лучше.

Продвижение и развитие продуктов и услуг – это важная и ответственная часть общего процесса поддержки продаж. Мы стоим на стыке взаимодействия технологий и людей, клиента и нашей компании. Я и мои коллеги знаем всё о том, как с помощью самых современных технологий, используемых в наших продуктах, эффективно противодействовать актуальным угрозам, а также помогаем нашим клиентам в решении их проблем. Как нам это удаётся? Каждый из нашей команды, не исключение и я, – это специалист своего дела, профессионал с уникальным набором hard и soft skills, позволяющим выполнять работу на высшем уровне. Так, я использую весь предыдущий более чем 8-летний опыт работы в сфере безопасности от специалиста – инженера в крупном интеграторе до специалиста по защите АСУ ТП и каждый день учусь чему-то новому.

Кроме того, работа в пресейле позволяет мне расширять географию, знакомиться с новыми интересными людьми и повышать свои компетенции. Так, за время работы в компании Positive Technologies (с 2017 года) я побывала в 10+ городах страны от Южно-Сахалинска до Калининграда, участвовала в 20+ мероприятиях по теме инфобеза, успешно совмещая всё это с изучением местных обычаев, достопримечательностей и, конечно, кухни.

Но для меня Positive Technologies – больше, чем просто работа: здесь можно найти единомышленников на любой вид хобби и активности, будь то участие в забеге, поход в горы или караоке.

POSITIVE TECHNOLOGIES

***Компания Positive Technologies** за 15 лет существования завоевала лидирующие позиции на отечественном и европейском рынке систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений.*

www.ptsecurity.com

CIS / № 4 (10) / 2019 / www.cismag.ru

«Ай Эн Ти»

Карина Романова
ООО «Ай Эн Ти»

ООО «Ай Эн Ти» является поставщиком ИТ-оборудования и программного обеспечения на территории Российской Федерации. Компания основана в 2012 году и является примером успешной молодой компании по продаже ИТ-оборудования и системной интеграции, созданной людьми с большим опытом работы в отрасли.

Головной офис ООО «Ай Эн Ти», где базируется «сердце» компании, и основные подразделения, обеспечивающие деятельность компании, расположены в Санкт-Петербурге. Также имеется обособленное подразделение, включающее в себя отдел продаж и склад (г. Москва).

Фактически отдел продаж компании заработал в июле 2012 году. Компания работала в формате четырёх продавцов и нескольких руководителей. На старте не было отдела закупок, склада, систем заявок и других поддерживающих систем.

Основной упор в продажах делали на активное оборудование: SFP, CWDM и DWDM. Первоначально продавали ТМ (торговую марку) Modultech, впоследствии была создана своя – ТМ NOVA. Продажи производились от задач клиентов, в связи с чем продуктовая линейка менялась и расширялась оборудованием, необходимым для операторов. Первые полгода были посвящены формированию клиентской базы и развитию компетенций продающего состава компании. Основные клиенты, с которых стартовала компания, – мелкие и средние провайдеры, проект по DWDM и Mail.ru.

Постепенно компания обрастала отделами, компетенциями, продуктовой линейкой. Появились отдел закупок, бухгалтерия, склад. Открылись офис и склад в Москве.

С 2014 года компания стала постепенно выходить на корпоративный рынок. Начались первые эксперименты по продвижению продуктов Nutanix, Kemp и др. Одним из запоминающихся реализованных проектов явился проект «Карвиль» (проектирование, поставка, пуско-наладка систем СКС и СКУД).

По итогам 2014 года были внедрены изменения в подсчёт маржи компании с учётом колебаний курса валют. Мы успешно преодолели сложный кризисный период.

С 2016 года в ООО «Ай Эн Ти» начались значительные системные изменения. Был создан технический отдел, организована работа по формированию регламентов и бизнес-процессов с целью повышения эффективности деятельности всей компании и каждого сотрудника в отдельности. Была создана система заявок, виртуализированы рабочие места, реформирован процесс работы с документами и базами данных, появился контроль движения товаров.

В настоящее время основными клиентами компании становятся корпоративные и государственные заказчики с индивидуальными задачами.

Компания работает на рынке системной интеграции с акцентом на инновационные решения. Совместно с партнёрами мы разрабатываем и внедряем программно-аппаратные решения, в том числе с использованием российских разработок, нацеленных на импортозамещение.

Основные направления деятельности компании:

- Разработка и внедрение проектов по созданию и модернизации сетевой и серверной инфраструктур, систем безопасности (СКУД и видеонаблюдение), систем связи (ВКС, IP-телефония, внутрикорпоративный обмен сообщениями, унифицированные коммуникации) и др.
- Производство серверного оборудования на базе Supermicro
- Аудит, модернизация и сопровождение текущей инфраструктуры
- Поставка и установка оборудования из Европы и Китая
- Умение найти на всех этапах работы наиболее эффективный способ решения задач, оптимальный по критерию цена/качество
- Индивидуальная работа с клиентами
- Глубокое погружение в проблему заказчика для нахождения наиболее приемлемого решения каждой конкретной задачи
- Готовность предложить каждому заказчику взаимовыгодные договорные условия
- Выполнение проектов «под ключ»

Основной продуктовый лист компании «Ай Эн Ти»:

- Серверное оборудование
- Системы хранения данных
- Сетевое оборудование
- Телефония
- IP TV
- ВОЛС
- ИБП
- Видеоконференцсвязь
- Организация рабочих мест
- Видеонаблюдение

Основными клиентами компании являются организации корпоративного сектора, государственные учреждения и ведомства, операторы связи.

Компания состоит из следующих структурных подразделений:

- Администрация
- Финансовый отдел
- Бухгалтерия
- Отдел продаж
- Тендерный отдел
- Отдел логистики и склада
- Отдел закупок
- Служба персонала
- Технический отдел
- Московский офис

В компании я руководитель финансового отдела, под моим началом функционирует отдел бухгалтерии.

Если выражаться формально, то моя роль в «Ай Эн Ти» – это обеспечение финансовой деятельности организации, но зачастую я ощущаю себя своего рода мамой. Ко мне можно подойти за советом и помощью. Любому сотруднику всегда будет оказана поддержка, начиная от сотрудника отдела продаж и заканчивая генеральным директором.

Все финансовые вопросы решаются через меня и мой отдел, параллельно я участвую в разработке стратегии компании, а также её стратегических целей и их воплощении в жизнь.

INNOVATIVE NETWORK TECHNOLOGIES

Компания ООО «Ай Эн Ти» *специализируется на комплексном оснащении IT-оборудованием операторов связи, корпоративного сектора, государственных учреждений и ведомств.*

Основными направлениями деятельности компании являются:
• Разработка и внедрение решений по созданию новых и модернизации текущих сетевой и серверной инфраструктур, систем видеонаблюдения, систем связи (ВКС, IP-телефония).
• Поставка IT-оборудования ведущих мировых брендов (вендоров) и ряда российских производителей.

www.innettech.ru

«Код Безопасности»

Ирина Налётова
Код Безопасности

Мы живём в век мощного и непрерывного потока данных. Информация поступает к нам не только из книг, газет, телевидения, радио: весь мир объединяет глобальный поток информации, циркулирующий в интернет-пространстве. Но каждый ли пользователь осознаёт, насколько важно защищать информацию, которую он получает или передаёт?

Только представьте, что было бы без защиты информации. Под ударом оказались бы все финансовые организации, информационные системы которые хранят данные о пользователях и их счетах. Злоумышленнику достаточно лишь получить доступ к виртуальным счетам вкладчиков, и он может стать миллионером. Банки, допустившие утечку конфиденциальной информации, не только дорого заплатят по счетам, но и понесут репутационный ущерб.

Я работаю в компании «Код Безопасности» – это российский разработчик сертифицированных средств защиты информации. Сегодня «Код безопасности» – это более 500 сотрудников, 4 российских офиса (в Москве, Санкт-Петербурге, Пензе и Анапе), более 1200 партнёров, свыше 32 тысяч государственных и коммерческих организаций заказчиков.

Компания разрабатывает аппаратные средства и программные продукты для обеспечения комплексной безопасности ключевых компонентов ИТ-инфраструктуры: защита конечных точек, сетевая безопасность, защита виртуальных сред и мобильных устройств, а также средства создания и проверки электронной подписи. Такой принцип позволяет заказчикам поэтапно развивать свою систему обеспечения информационной безопасности.

Аналитик-маркетолог – это специалист, которые совмещает два направления деятельности: поиск оптимальных решений классического маркетинга и анализ текущей ситуации. Именно эту должность я занимаю в компании.

Ещё Натан Майер Ротшильд сказал: «Кто владеет информацией, тот владеет миром». Одна из моих основных задач – работа с информацией. Ежедневно через меня проходит огромный объём данных, которые необходимо проанализировать, построить прогноз и выбрать правильную маркетинговую стратегию как для продвижения отдельных продуктовых линеек, так и для развития компании в целом.

Самыми сложными и одновременно самыми интересными в моей работе являются продуктовые маркетинговые исследования. Каждый такой проект длится несколько месяцев и представляет собой огромный аналитический труд. Основная идея исследования состоит в выявлении ключевых рисков информационной безопасности в организациях различных отраслей и помощи ИБ-специалистам в выработке правильной стратегии защиты данных. Получаешь огромное удовлетворение, когда проходишь длинный путь от разработки анкеты, анализа цифр до оформления отчёта с выводами, публикуешь исследование, а потом читаешь письма благодарности о том, что материал очень помог.

На аналитика-маркетолога возложена огромная ответственность, ведь от точности его прогнозов в определённой степени зависит будущее компании, выбор пути её перспективного развития. Мои знания в сфере экономики и маркетинга, структурное мышление, хорошие память и логика, готовность сразу погрузиться в изучение незнакомой ранее отраслевой специфики, умение применять аналитические инструменты помогают компании не только решать локальные бизнес-задачи, но и выбрать стратегически верный курс развития.

КОД БЕЗОПАСНОСТИ

Компания «Код Безопасности» *ведёт свою деятельность на основании девяти лицензий ФСТЭК России, ФСБ России и Министерства обороны Российской Федерации.*

www.securitycode.ru

«Axoft»

Я работаю в компании Axoft 2.5 года. Сейчас занимаю должность solution sales manager – специалиста по подбору решений информационной безопасности.

Усачёва Мария
Компания «Axoft»

Иногда даже сравниваю себя с терапевтом, так как моя работа заключается в том, чтобы правильно услышать потребности заказчиков и предложить им решения «закрывающие боль». Не секрет, что риски есть не только у крупных компаний с миллиардным оборотом, но и у нас – обычных пользователей мобильных приложений, держателей банковских карт и просто людей, привыкших искать любую информацию в Internet.

На сегодняшний день я вижу всю сложность защиты от современных угроз. Проекты, которые мы реализовываем вместе с нашими партнёрами, закрывают все основные потребности и задачи рынка: от установки антивирусов до помощи в организации SOC. А ведь когда-то вся информационная безопасность для меня заключалась в скачивании ключа из интернета для продления домашнего антивируса (да, теперь мне за это немного стыдно).

Очень ценю слаженный и профессиональный коллектив, в котором я работаю. И если продолжить проводить параллель с врачебной практикой, то я так же, как и терапевт, после первичной диагностики передаю партнёров и клиентов в надёжные руки узких специалистов для дальнейшего тестирования. Только работая в ИТ, мы обследуем не человеческий организм, а ИТ-инфраструктуру партнёров и заказчиков и каждому прописываем свой «рецепт» – EDR, DLP, SOAR или AntiAPT-решения… В информационной безопасности много направлений.

Люблю свою работу за возможность постоянно совершенствовать знания, знакомиться с интересными людьми и участвовать в глобальных проектах.

Немного о компании

Axoft – глобальный сервисный ИТ-дистрибутор. Ежедневно аккумулируя международный и отечественный бизнес- и ИТ-опыт, Axoft выступает центром компетенции по вопросам построения информационной безопасности, совершенствования ИТ-инфраструктуры и трансформации её в «облака». В том числе выступает экспертом по теме импортозамещения в ИТ, использования практик Open Source и DevOps. Ежемесячно проводит около 5000 продуктовых, технических и бизнес-консультаций.

В её портфеле есть решения для государственных компаний, коммерческих корпораций, представителей малого и среднего бизнеса. Axoft сотрудничает с более 1500 ИТ-производителей по всему миру, в т. ч. с технологическими лидерами из квадрантов Gartner и представителями реестра российского ПО.

Компания предлагает глубокие продуктовые и технические компетенции, полностью поддерживая ИТ-проекты, которые партнёр реализует со своими заказчиками. Она проводит аудит ИТ-инфраструктуры, помогает в пре-сейле, защищает проекты перед заказчиком, предоставляет тестовое «железо», занимается внедрением и последующей технической поддержкой в режиме 24/7.

Компания Axoft представлена в 27 городах и 9 странах мира ипоказывает ежегодный прирост «выше рынка»: в 2018 FY оборот превысил 13,5 млрд долларов, что на 25% выше предыдущего года.

AXOFT

Компания «Axoft» *– сервисный IT-дистрибутор, работающий на рынке России и ВЕЦА.*

axoftglobal.com

«АТОЛ»

Екатерина Чурзина
Компания «РегионКом»

Компания «АТОЛ» – ИТ-лидер в области автоматизации ритейла и сферы услуг. В 2016 году компания вошла в Топ-5 престижного рейтинга «Крупнейшие поставщики ИТ для розницы». А уже в 2017 году компания заняла 1 место рейтинга «Крупнейшие поставщики ИТ в рознице».

Компания «АТОЛ» была основана Алексеем и Ириной Макаровыми в 2001 году. Она специализируется на разработке и поставке оборудования и программного обеспечения для автоматизации front-офиса сетевого и независимого ритейла (food и non-food), кафе, ресторанов, гостиниц, сферы услуг и других областей предпринимательского рынка. Компания «АТОЛ» – это собственное производство и разработка контрольно-кассовой техники, в том числе облачной, программного обеспечения для неё и огромное количество других уникальных digital-решений, оптимизирующих ведение бизнеса.

В числе решений АТОЛ:

- контрольно-кассовая техника онлайн;
- смарт-терминалы и ньюджеры;
- транспортные модули для Единой государственной автоматизированной системы с целью контроля за производством и оборотом алкоголя (ЕГАИС);
- POS-системы, 2D-сканеры, весовое оборудование, принтеры чеков и фискальные регистраторы;
- широкий спектр программного обеспечения.

Партнёрская сеть АТОЛ насчитывает более 800 компаний во всех федеральных округах России.

В самом сердце компании «АТОЛ» находится её команда, а если быть точнее, команда мечты! Люди, работающие здесь, являются клетками этой уникальной системы! Большой, но сплочённый коллектив АТОЛ с распростёртыми объятиями принимает новых героев в свои круги! Молодые специалисты АТОЛ окружены заботой и вниманием с первых дней работы.

Множество мэссенджеров и корпоративных досок, чатов, совместного обсуждения увлекательных и безумно интересных задач – все эти активности не дадут приуныть и заинтересуют общим процессом! Быть профессионалом в АТОЛ – это интересно и перспективно! Мы любим свою компанию, для сотрудников АТОЛ – это вторая семья!

АТОЛ Онлайн

Компания «РегионКом» *успешно работает на рынке ИТ, реализуя проекты и оказывая услуги клиентам.*

www.regioncom.ru

eToken

Продукты линейки eToken –
основа инфраструктуры информационной
безопасности современного предприятия

etokenstore.ru

Мерцающие суперструктуры

Выставка «Мерцающие суперструктуры / Oscillating Superstructures». Совместная персональная выставка саундартистов Сергея Филатова (Россия) и Якоба Ремина (Jacob Remin, Дания). Сергей Филатов и Якоб Ремин имеют общий интерес к физической стороне медиа и современного саундарта. Они оба создают объекты, манифестирующие себя в пространстве инструментов, композиций и инсталляций. Художники исследуют и модифицируют технологические компоненты, фокусируясь на звуке. Они предлагают пространство для диалога и сопротивления в мире, навязывающем нам быстрые реакции визуальности. Художники настаивают на замедлении и вслушивании, на создании новых иерархий, идущих против течения.

Пространственная корреляция

В рамках проекта «Искусство звука» открывается выставка «Пространственная корреляция / Spatial correlation». В совместном проекте «Пространственная корреляция/Spatial correlation» медиахудожники Сергей Филатов и Якоб Ремин подготовили многоканальную инсталляцию, создающую звуковую среду на основании взаимовлияния авторских полевых записей (электромагнитные излучения сигналов устройств передачи беспроводного интернета) и медиа-объекта «MetaRotator», созданного Сергеем Филатовым по принципу электромагнитной индукции. Проект был впервые презентован в 2018 году в Inter Arts Center (Мальмё, Швеция). Сергей Филатов – полевые записи, DIY объект-генератор Якоб Ремин – программирование (Max/MSP).

Департамент культуры города Москвы

ОБЪЕДИНЕНИЕ ВЫСТАВОЧНЫЕ ЗАЛЫ МОСКВЫ ЭЛЕКТРО МУЗЕЙ

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

ИТ-прогноз до 2045 года: цифровое человеческое бессмертие

2019 год выдался весьма интересным и разнообразным на события в ИТ-мире!

С одной стороны, ИТ-гиганты радовали нас своими новыми решениями и продуктами, с другой стороны, появление сотен новых стартапов по всем фронтам не давали пытливым умам и инвесторам покоя, а с третьей – прогнозы учёных и футурологов порой вводили в шок.

Как бы то ни было, мир меняется, и мы меняемся вместе с ним. Удалившись от повседневной рутины, закрыв глаза, хочется представить новые перспективы и подумать о ближайшем будущем.

Что нас ждёт в этот беспокойный 21 век?

Зачем все эти странные и порой непонятные «гаджеты» и «виджеты»?

Зачем столько усилий отдавать работе, если скоро всё за людей будут делать роботы и искусственный интеллект?

Чем мне вообще заниматься в этом постоянно меняющемся «цифровом» мире?

Немного фантазии и наблюдательности, и с большей долей вероятности мы с вами можем заглянуть в ближайшее будущее, в мир развития технологий четвёртой промышленной революции, а самое главное, интуитивно ощутить слабый ветерок «цифровых» перемен.

Сейчас появилось много направлений развития технологий, порой даже кажущихся нереальными и немного безумными. Но, что, как ни человеческая мысль, является двигателем реального прогресса или ключом к вратам бесконечных трансформаций.

Последние двадцать лет работы в области информационных технологий, несомненно, отразились и на моём мироощущении и мировосприятии. Несомненно, у меня сформировалось устойчивое ощущение того, к каким высотам стремится наше с вами «цифровое» будущее. Давайте посмотрим...

- 2025 – Прежде всего это формирование и развитие законодательства и нормативно-правовой базы в области взаимодействия и сосуществования роботов, искусственного интеллекта и человека. Активное становление отрасли робототехники в РФ и внедрение новых решений во всех отраслях экономики.
- 2026 – Имплантируемая электроника и развитие микрокомпьютерной техники. Активное развитие Интернета вещей в РФ. Появление новых молодёжных субкультур (например, возможно возрождение идеи «киберпанка»).
- 2027 – Новые источники альтернативной энергии. Трансформация мировых экономик и активная «цифровизация» экономики РФ. Особая роль в России будет уделяться развитию науки, созданию новых технологий и продуктов на базе лучших мировых практик.
- 2028 – Широкое применение нано-, био-, нейро- и иных технологий в промышленности, медицине и других отраслях экономики РФ. Развитие квантовых технологий в области физики, химии и материаловедения для создания устойчивых квантовых компьютеров.
- 2029 – Широкое применение 3D-принтеров для печати человеческих органов. Развитие регенеративной и наномедицины.
- 2030 – Интернет везде. Появление и развитие альтернативных независимых глобальных сетей, построенных на принципиально других научных подходах. Широкое развитие «киберспорта» по всему миру.
- 2031 – Искусственный Интеллект (ИИ) станет на порядок совершеннее. Широкое применение ИИ в медицине, образовании и других отраслях. Первое преступление, совершённое ИИ. Первые глобальные кибервойны за владение рынком ИИ.
- 2032 – Объединение Интернета и ИИ. Трансформация поисковых систем. Появление новых интерфейсов доступа в глобальные сети.
- 2033 – «Киборгизация» – новый тренд в увеличении продолжительности жизни человечества. Развитие субкультуры «киберпанка».
- 2034 – Применение ИИ во всех отраслях экономики.
- 2035 – Новые открытия в области изучения человеческого мозга.
- 2036 – «Программируемая биология». Новый скачок в создании квантовых компьютеров и рост «квантового объёма» – квантовой мощности вычислений. «Первое квантовое превосходство».
- 2040 – «Киборгизация 2.0». Применение нанороботов для трансформации человеческого тела. Трансформация субкультуры «киберпанка».
- 2041 – Автономный транспорт и логистика на искусственном интеллекте во всех отраслях экономики РФ.
- 2042 – Новые достижения в развитии технологий виртуальной реальности.
- 2043 – Появление принципиально новых нанобиоинтерфейсов. «Стыковка» мозга с компьютерными нейросетями. Новый уровень управления «искусственными» протезами и телами. «Киберпанк», «киберспорт» и «кибервойны» – это не тренд, а реальность.
- 2044 – Очередной скачок в развитии ИИ. Появление ИИ, созданных самим ИИ. «Вирусный ИИ». Самостоятельное объединение разных версий ИИ в псевдосоциальные группы.
- 2045 – «Пятая промышленная революция» и «Цифровое человеческое бессмертие». «Первое квантовое превосходство». Интеграция ИИ с квантовыми компьютерами.

Подводя промежуточный итог, отметим, что в ближайшие десять – тридцать лет наше с вами общество претерпит существенные трансформации. Тот социальный и экономический уклад, который мы наблюдаем сейчас, кардинально изменится, и, пожалуй, пиком этих изменений в ближайшие 25 лет станет «цифровое человеческое бессмертие».

Вопрос цифрового человеческого бессмертия – это уже не вопрос: быть или не быть. Ответ для человечества на сегодняшний день очевиден – однозначно, быть!

Как мы с вами понимаем, этот вопрос не новый и будоражит умы людей уже не одно столетие. Но сегодня мы

как никогда близко подходим к ответу на него.

Кроме того, когда речь идёт о новой технологической революции и буквально буму на создание новых технологий как следствие этого процесса, возникают новые вопросы, в том числе, какие из технологий четвёртой промышленной революции позволят нам прожить хотя бы лет сто, двести или существовать как можно дольше?

Возможно ли это?

В теории, очевидно, да!

Как бы это могло быть?

Пожалуй, на этот вопрос ответить совсем не сложно.

С точки зрения информациологии или информационных технологий, человек представляет собой некую систему, в которой собирается, обрабатывается и хранится масса разнородной структурированной и неструктурированной информации. Всю эту информацию мы называем «наша память», «наш жизненный опыт» и т.д. Кроме того, человек – это ещё уникальная система, которая «творчески» и беспрерывно формирует алгоритмы получения, обработки и хранения этой информации, и эти алгоритмы тоже хранятся внутри нас.

Уникальность нашего мозга состоит ещё и в том, что он способен «забыть» не только некие данные, но и при необходимости забыть сами алгоритмы их получения. Тем не менее в случае необходимости он способен в любом возрасте учиться и легко формировать новые алгоритмы поиска решения, а также собирать, обрабатывать и хранить новые данные. И так далее.

Но, возвращаясь к вопросу цифрового человеческого бессмертия, скажем, что всё не так просто, как может показаться на первый взгляд…

Наш с вами мозг и нервная система – это суперкомпьютер со своей системой интерфейсов. За обработку информации в нашем мозге отвечают порядка 86-100 млрд нейронов (нейронных клеток), которые меняют своё состояние до 50 раз в сёк. Число возможных состояний нашего мозга = $10^{1000000}$ (количество возможных комбинаций возбуждения или торможения нейронов), тогда как количество атомов во Вселенной = 10^{80}.

Кроме того, на сегодняшний день никто не может дать ответ на вопрос, сколько экзабайт (10^{18}) или йоттабайт (10^{24}) данных и в какой форме хранится в нашем мозге.

Исходя из этих скромных данных, можно сделать вывод: появление настоящего искусственного интеллекта возможно лишь тогда, когда человечество создаст квантовый компьютер, сопоставимый по своим вычислительным мощностям с нашим мозгом, и вывод второй: полноценное «цифровое человеческое бессмертие» возможно лишь тогда, когда будут созданы квантовые носители информации.

Тем не менее современные технологии четвёртой промышленной революции не стоят на месте. Давайте представим себе ситуацию, что вычислительные, нано-, био-, нейро- и другие технологии к 2045 году достигли такого уровня, что способны оцифровать и сохранить наше сознание, а также перенести все эти «йоттабайты» данных на внешний носитель или, например, сразу в другое тело (телом может служить и некая гибридная биомеханическая система или робот, или искусственно выращенный или распечатанный на 3D-принтере человек). И число таких переносов может быть бесконечное число раз.

Вот вам и цифровое бессмертие…

Но!

Тут мы с вами сталкиваемся ещё с одной трудностью, которая заключается в том, что если перенесённый разум на «внешний носитель» или в виртуальную среду не сможет взаимодействовать с внешним миром, то фактически для нас этот разум или человек всё равно что умер! Об этой проблеме говорил ещё Станислав Лем в «Диалогах» (1948-1950 годы) и «Сумме технологии» (1963 год).

Что, собственно, и происходит с нами сейчас. На протяжении тысяч лет религия разных народов и культур предоставляла нам «интерфейс», причём односторонней связи с теми мирами, куда уходит наши сознание, разум или душа после смерти. И на протяжении тысяч лет никто из живущих людей посредством религии не смог получить обратной связи из тех миров. По моему скромному мнению, в ближайшие сто лет все мировые религии сильно трансформируются. Неизбежно, что под влиянием новых технологий разовьются сотни новых субкультур, а наука займёт место «новой религии», которая станет способна предоставить всему человечеству «двунаправленный интерфейс» с новыми мирами, будь то виртуальная реальность или параллельная вселенная, или даже Рай, который, несомненно, существует!

Но не будем задерживаться на трансцендентных «темах», и устремим взгляд в 2045 год, где будут созданы новые нано-, био- и нейроинтерфейсы, способные соединить наше сознание с любой информационной средой и внешним миром. И вот здесь, помимо тысяч инженерных сверх задач переноса, хранения и обработки информации нашего сознания, скрываются новые вопросы, которые последуют за этими техническими задачами, например:

Будет ли это «новое существо», в которое поместили наш разум, нами? Или копией нас с теми же знаниями и опытом?

В какой момент времени осуществить перенос сознания: при жизни или, например, в первые пять минут после смерти, как это предлагают некоторые «энтузиасты»?

Сможем ли мы принять свою новую реальность или сущность, кем бы ни стали: киборгом, андроидом, роботом или каким-нибудь гибридом?

С философской точки зрения, наше тело лишь временное убежище или дом для сознания, и рано или поздно это сознание – наша душа найдёт себе новый дом.

Немаловажен и вопрос, как долго человек сможет жить на земле в своём новом теле? Готов ли наш мозг существовать столетия, а сознание быть бессмертным?

Интересным и открытым остаётся вопрос: а что если копию сознания поместить сразу в несколько тел? Будем ли мы ощущать себя единым целым, единым коллективным разумом или получим множество «новых людей»?

И совсем интересной станет ситуация, когда наше сознание будет по-

мещено не в человекоподобное тело, а, например, в робота-паука или робота-рыбу… А если сознание поместят в ящик с манипулятором и у нас не будет возможности общаться с внешним миром, а лишь исполнять приказы, не сойдём ли мы с ума, находясь в таком заточении?

И, наконец, мы добрались до самого главного вопроса: смогут ли нас принять наши близкие люди в любом новом воплощении? Будем ли мы для них тем же прежним дорогим и любимым человеком?

И вот тут мы сталкиваемся с огромным числом новых вопросов, на которые человечеству в ближайшие десятилетия только предстоит ответить и не один раз!

На сегодняшний день, пожалуй, одним из самых перспективных направлений работы, с теоретической точки зрения, является процесс переноса человеческого сознания в виртуальную реальность.

Как вам, возможно, известно, уже не первый год идут активные работы как в направлении развития технологий создания виртуальной реальности, так и работы по созданию аппаратной реализации человеческого мозга. И лет этак через двадцать – тридцать вполне возможен процесс последующей выгрузки наших с вами «сущностей» на новый цифровой носитель, который будет существовать уже в нашей реальности, в нашем мире.

При решении вопроса цифрового бессмертия возникает ещё одна интересная инженерная задача: как уже имеющиеся знания и опыт, собранные человечеством, поместить в человеческий мозг, минуя годы штудирования книг и накопления жизненного опыта. Ведь без её решения мы не сможем жить вечно!

Все знания мы получаем из внешнего мира постепенно, и в наше сознание они помещаются не сразу. Они как бы остаются в буферной зоне, структурируются и оттачиваются нашим сознанием порой даже не один день или год. Совершенствуются и уже потом формируют наш опыт. Можно фигурально сказать: знания помещаются в «библиотеку», или на «склад», откуда мы их берём, используем, добавляем и обновляем в течение всей нашей жизни.

Этот процесс сложный и по большей части индивидуальный для каждого человека. Проблема заключается в том, что на сегодняшний день люди не знают, как и в каком формате хранятся знания у нас в голове, а тем более как их упаковать и передать в мозг другого человека.

Кроме того, в настоящее время не созданы нейро- или биоинтерфейсы способные передать информацию из некого «хранилища» непосредственно в наш мозг.

Ещё сложнее дела обстоят с опытом человека.

Представьте себе, что инженеры и учёные справились с этими задачами.

Они научились буквально, как говорят айтишники, закачивать или «заливать» знания в огромных объёмах в наш мозг…

Что же будет с нами?

А будет, пожалуй, вот что…

Человек превратится в некого «супервсезнайку» или суперчеловека.

Представьте себе такую ситуацию: вы повар и получили знания по карате. Теперь вы знаете все приёмы и, конечно, захотите их испытать. Оп, бац, вы махнули рукой, ногой и ещё раз ногой. Что после? С большей долей вероятности вы покалечитесь, сломав себе руку или порвав все связки. Ваш мозг будет знать, как и что делать, но тело не будет к этому готово.

Пример другой: вы получили знания по психологии и все знания по медицине за всю историю человечества. И что? Да вот что: с вами как минимум случится синдром студента 3-го курса медакадемии. Вы попросту примерите все болезни на себя, а так как полученные знания ничего не имеют общего с вашим опытом, то, скорее всего, подумаете, что больны сразу всеми болезнями на свете, и есть вероятность, что сойдёте с ума. То есть в результате человек попросту поломается…

А вот ещё одна инженерная задача: какой объём информации будет способен получить человеческий мозг через нейроинтерфейс, чтобы не аннигилировать? Чтобы человек смог весь объём информации принять, обработать и систематизировать и при этом не сойти с ума? Никто не знает…

Да, пока все эти проблемы и задачи не решены, конечно, нельзя говорить о цифровом бессмертии в полном его понимании.

Тем не менее, по моим оценкам, к 2045 году уровень криотехнологий, генной инженерии, технологий «киборгизации», регенеративной медицины и робототехники достигнут своего пика, что позволит людям значительно повысить качество и продолжительность своей жизни. Такое баловство, как «биохакиг» и иные истории с трансплантологией микрочипов и микрокомпьютеров растворятся в субкультуре киберпанка без остатка. Сомневаетесь? В Библии сказано: «И он сделает то, что всем: малым и великим, богатым и нищим, свободным и рабам положено будет начертание на правую руку их или на чело их, и что никому нельзя будет ни покупать, ни продавать, кроме того, кто имеет это начертание, или имя зверя, или число имени его. Здесь мудрость…» (Откр. 13:16-18).

Параллельно с этими процессами люди научатся переносить человеческое сознание не только в цифровую виртуальную среду, но и на новый биологический носитель, будь то искусственно выращенный человеческий мозг или клон человека, например распечатанный на 3D или 4D-принтере.

В ближайшем будущем технологии позволят создавать новые материалы, из которых будут созданы новые носители информации, которые в свою очередь станут прототипами нашего с вами мозга. Таким образом, уже к 2045 году человечество научится переносить свои «сущности» в «новые тела».

Хорошая новость для человечества заключается в том, что мы с вами в шаге от цифрового бессмертия, плохая – что у нас по-прежнему остаются тысячи неразрешённых вопросов…

Новых свершений и хорошего вам Нового 2020 года!

Александр Чесалов
Директор по развитию ООО «Программные Системы Атлансис»,
Член Совета ТПП РФ по развитию информационных технологий и цифровой экономики, д. т.н., Член-корр. РАЕН

www.чесалов. рф

Цифровая трансформация и современная экономика

Современная экономика не эффективна

Почему мы наблюдаем большие преобразования во всех сферах жизни за счёт мощного развития науки и техники, особенно информационных технологий (ИТ), а с другой стороны, продолжается примитивная погоня бизнеса за прибылью, как 200 лет назад? Может, это естественно?

Думается, нет, и не только в силу архаизма, а в результате негативного влияния на состояние экономики. Как правило, в этом случае наблюдается противоречие общественных и корпоративных интересов, потому что сегодня уже не работает принцип «чем лучше бизнесу, тем лучше обществу». Выгодно бизнесу в ущерб интересам общества. Если в погоне за прибылью травят сотни людей, то не о выгоде надо говорить, а о преступлении.

И вообще представляется, что некоторые рыночные принципы в России доведены до абсурда. Конкуренция ради конкуренции, конкуренция как самоцель. Зачастую это создание видимости, хотя в действительности никакой конкуренции нет. Главное – рынок, прибыль, наличие миллиардеров, а к чему это приводит уже сегодня и что станет в будущем, адептов рынка не интересует. По меньшей мере, можно говорить о слабой адаптивности рынка, особенно в части решения социальных вопросов.

В чём причина такого положения? Прежде всего, это проявление нарушения объективно действующего принципа соответствия уровня производительных сил производственным отношениям, а игнорирование этого принципа со стороны научной общественности свидетельствует об отставании экономической мысли.

Кроме того, сказывается влияние тех, кто владеет деньгами, – они навязывают мысль, что другого быть не может и это чуть ли не от бога. К сожалению, многие учёные «обнаучивают» эти догмы, ибо они ищут не истину, а выгоду, отсюда и отставание экономической теории от практики. А истина в том, что надо сохранить жизнь на планете, сохранить природу и человека. При этом не только для одного миллиарда избранных, а для всех. Другими словами, надо отказаться от современной неэффективной экономики и становиться на путь устойчивого развития.

По определению Международной комиссии по окружающей среде и развитию, устойчивое развитие – это такое развитие, которое удовлетворяет потребности настоящего времени, но не ставит под угрозу способность будущих поколений удовлетворять свои собственные потребности.

Оно включает в себя два ключевых понятия:

- **понятие потребностей, в частности потребностей,** необходимых для существования беднейших слоёв населения, которые должны быть предметом первостепенного решения;
- **понятие ограничений,** обусловленных состоянием технологии и организацией общества, накладываемых на способность окружающей среды удовлетворять нынешние и будущие потребности.

Но кто заинтересован в этом? Правительства как носители общественных, государственных интересов – да, если бы они не находились под влиянием транснациональных компаний, которые стремятся максимизировать ту же прибыль, невзирая на войны, болезни, голод, разрушение планеты. Будет ли Правительство РФ реализовывать концепцию устойчивого развития?

Спрашивается, как сами творцы-идеологи оценивают эту ситуацию, беспокоит ли их, что мир на краю пропасти, или они, по-видимому, рассуждают, что их интересов это не коснётся, а люди не нужны – их заменят роботы? Численность населения надо сокращать, и в этом выход из тупика – к такому выводу ведёт сегодняшняя капиталистическая модель, создавая пропасть между бедными и богатыми: богатые должны богатеть, бедные – беднеть.

Никакими экономическими теориями нельзя объяснить, например, плоскую шкалу налога на доходы физических лиц в России. Объяснение одно: если ты богатый – тебе всё позволено, а бедные – это отбросы общества, они никому не нужны и сами виноваты в создавшемся положении. Да, они виноваты в том, что терпят такое, не протестуют против этой чудовищной несправедливости.

Надо отметить, что если на Западе хоть и говорят о балансе интересов, о социальной справедливости, то в России речь может идти о попытках социально ориентированного государственного бюджета, социальных подачках и т.п. И всё это под прикрытием рынка – если ты рыночник, то владеешь истиной.

Вместе с тем такая рыночная экономика тупиковая, она зиждется на увеличении спроса, который поддерживается искусственно. Это затратная экономика: чем выше затраты, тем больше ВВП. Это к тому же разрушительная экономика, её время прошло, мир уже насы-

тился её товарами. На планете нет больше ресурсов для такой расточительной экономики, они жёстко ограничены. Из-за искусственного увеличения спроса большая часть произведённых товаров или используется на пять процентов, или просто выбрасывается на свалку.

И это не циклический кризис перепроизводства, это перманентное явление. Такое положение может являться причиной того, что сегодня есть проявления отрицательной доходности на капитал. Становится невыгодно владеть материальным активом, он превращается в обременение.

Как вывести экономику из тупика?

Не вдаваясь в дальнейшие рассуждения и с учётом выше изложенного, возникает вопрос: «Какой выход?» Смогут ли, допустим, современные достижения науки и техники, в частности ИТ, изменить положение, вывести экономику из этого тупика?

Такая постановка вопроса может показаться слишком смелой, ведь до недавнего времени многие экономисты ещё сомневались, собственно, в состоятельности самих ИТ, в их эффективности: дают ли они повышение производительности?

Разработано множество методик установления эффективности информационных технологий, на основе которых определялся эффект от внедрения ИТ во многих отраслях. Но произошла облачная революция в ИТ, расходы на них резко уменьшились, и уже такой вопрос не стоит, как не стоит вопрос, например, надо ли пользоваться электричеством. Задача в выборе оптимального варианта использования или применения ИТ (SaaS, IaaS, Paas или др.). Существенное удешевление ИТ-услуг послужило стимулом цифровой трансформации.

Был период в управлении экономикой, когда крайне остро стояла задача нахождения оптимального соотношения «централизация – децентрализация» – это, как известно, одна из главных проблем управления. И она с помощью ИТ была успешно решена. Решаются и другие задачи.

Сегодня есть примеры, когда на основе ИТ возникают новые бизнес-модели и направления в экономике, одно из них – шеринговая экономика, или экономика совместного использования. Благодаря ИТ удаётся свести воедино спрос и предложение в реальном времени и максимизировать использование основных средств производства.

Когда продаётся услуга на проезд в автомобиле (пример – Uber), повышается коэффициент его эксплуатации с 0,05 до 0,45. И не только это, такая услуга в целом удешевляется. Да, целевая функция при такой модели – получение прибыли – остаётся, но это не противоречит общественным и личным интересам (баланс – личные, корпоративные, общественные).

Другой пример: интернет вещей и его дальнейшее развитие – промышленный интернет как модель идеальной системы взаимодействия поставщика и потребителя, которая в каждый момент времени стремится к наибольшей эффективности. С одной стороны, за счёт принципа самообслуживания потребитель имеет возможность получить нужный продукт в необходимом ему объёме и требуемого качества в конкретный момент времени. С другой стороны, производитель за счёт гибкого масштабирования производства для создания заказанного продукта (услуги) использует ровно столько и такого ресурса, сколько и какого необходимо.

Электронная торговля, которая принципиально отличается от традиционной в смысле оперативной обратной связи с производителем (изготовление товара по индивидуальному заказу), и другие модели. Преобладающим становится не продажа товаров, а предоставление услуг. Потребитель покупает не оборудование, а его функцию. Это позволяет смягчить вопрос реализации товара, избежать перепроизводства. Такие модели, в частности экономика совместного потребления, во многом снимают остроту разорительной экономики за счёт снижения издержек и уменьшения негативного влияния на окружающую среду.

Совместимы ли искусственный интеллект и рыночные отношения?

Но что это: предтеча новой экономической модели или только усовершенствованная старая рыночная модель? Да, можно видеть, что с помощью ИТ совершенствуются основные рыночные функции, в определённом смысле они автоматизируются. Дело в том, что новые бизнес-модели экономики, как и совершенствование основных рыночных функций, в целом направлены на сохранение природы, экономию ресурсов, что в конечном счёте обеспечит устойчивое развитие как путь сохранения человечества. Происходящая цифровая трансформация является залогом устойчивого развития. Это важный позитив.

Но это только начало. Уже сегодня возможности влияния ИТ не только на экономику, но и на саму экономическую модель велики и в дальнейшем будут только неуклонно расти. Огромные достижения в области обработки больших данных позволяют реализовать полную персонализацию потребления (учесть текущие и будущие потребности каждого человека). А это, в свою очередь, позволит проводить непрерывное моделирование экономических процессов в реальном времени и на этой основе прогнозировать и решать многие рыночные проблемы: инерционность, неспособность видеть перспективу, кризисы.

По прогнозам аналитиков, 80% существующих бизнес-процессов и моделей будет через пять лет изменено или отменено. Такие революционные изменения побуждают говорить не только о совершенствовании рынка или его существенной модификации, но и о зарождении возможной альтернативы рынку.

Если уже сегодня некоторые функции рынка могут перейти к ИТ – регулирующие (большие данные и моделирование), посреднические (промышленный интернет, электронная торговля), контролирующие (непрерывный мониторинг экономических процессов в реальном времени), то в будущем такой переход в конечном счёте может привести к отмиранию данных функций как таковых. Потому такое предположение кажется вполне оправданным.

Возможно, сегодня рано говорить об этом, но с дальнейшим развитием ИТ и искусственного интеллекта (ИИ) появление альтернативы рынку станет реальностью. Очевидно, что решение проблемы лежит

в плоскости ИИ: по какому пути он пойдёт, кем будет контролироваться и направляться? Возникают вопросы: как отнесётся к этому элита? Будет ли избран путь устойчивого развития или произойдёт отказ в пользу уменьшения населения с дальнейшей простой роботизацией? Так как финансирование развития ИТ, и особенно ИИ, находится в частных руках (одно из разительных противоречий современной экономики), этот выбор имеет принципиальное значение: то ли ИИ будет служить всему человечеству во имя его процветания, то ли он станет инструментом порабощения, усугубления неравенства и несправедливости.

И вообще уместен вопрос: совместимы ли ИИ и рыночные отношения? Ведь ИИ предполагает самосовершенствование, а рынок его тормозит, как зачастую и другие новые идеи. Не будет ли ИИ тесно в рамках сегодняшних рыночных отношений? Рынку нужен постоянный спрос, и компьютерные фирмы, например, пытаются его формировать, но ИИ сам может определять этот спрос. Подход к основному рыночному принципу «спрос – предложение» меняется, это уже не прерогатива рынка, ИИ формирует спрос и сам становится потребителем.

Есть ли альтернатива рынку?

Если речь идёт о возможной альтернативе рынку, то может возникнуть вопрос о конкуренции как одном из стимулов научно-технического прогресса. Действительно, большие успехи в развитии информационных технологий связаны с конкуренцией, но в недрах ИТ быстро развивается свободное программное обеспечение (ПО), которое может занять доминирующее положение. А если так, то смысл конкуренции на этом поле отпадает.

Важная черта сегодняшнего мира – открытость. Соответственно, роль и место конкуренции меняются. Не разорительная конкурентная борьба ради максимизации прибыли, а созидательная борьба за новые идеи, технологии, методы управления, что, разумеется, предполагает различные взгляды и подходы, всячески отказ от монополизма. В рамках цифровой трансформации уместно ставить вопрос о переходе от конкуренции к кооперации.

И если в целом говорить о проблемах развития ИИ, то стоит задача создания дружественных информационных технологий, которые станут сильным и полезным инструментом доступа к информационным ресурсам и другим сервисам, будут способствовать росту производительности общественного труда. Необходимым условием создания дружественных ИИ является отказ от ориентации их на максимизацию прибыли, так как в таком случае только усугубятся рыночные проблемы.

Возможно, этот выбор носит больше политический характер и требует всесторонней проработки с привлечением учёных, политиков, бизнеса и общественности, но проработка его весьма актуальна.

Широко распространено мнение, что сегодня мы живём в информационном обществе, что набирает силу цифровая экономика, где на первом месте информация и знания. Представляется, что пока это не так – ни знания, ни информация не имеют самостоятельного значения, они в конечном счёте превращаются в инструмент добывания денег.

Очевидно, дальнейший бурный рост технологий – нано, био, инфо – изменит ситуацию в сторону знаний, так как мир всё больше становится интеллектуальным и технологичным, виртуальным.

Основной ценностью становятся нематериальные активы, уже сегодня они составляют более 70% активов предприятия. Создаётся основа для реального построения информационного общества и, как следствие, возникновения новой элиты (например нетократия), которая фактически может владеть этими активами, а не деньгами или акциями, ибо без знаний (которые в головах людей) активы ничего не будут стоить.

Может быть, критерием станет не прибыль, а получение новых знаний, технологий. Если принцип «капитал создаёт капитал» не будет работать (а сегодня это уже отчётливо проявляется), то есть ли смысл выставлять прибыль как цель?

Как один из инструментов определения эффективности – да, но не более. Уже сейчас есть немало некоммерческих организаций, которые успешно реализуют многие проекты различной степени сложности и важности.

Возможно, критерием успешности в обществе будет становиться умение как можно эффективнее использовать ресурсы, а не владеть как можно большим их количеством. Повышение устойчивости бизнеса, достижение оптимальных, научно обоснованных пропорций, баланс интересов – всё это могут дать знания, информация, новые технологии.

Такая тенденция означает изменение структуры занятости в пользу создания всё большего числа рабочих мест, связанных с выполнением человеком творческих задач, а не рутинных функций, с последующей заменой тех, кто их выполняет, – на роботов. А основным капиталом будет человек с его знаниями.

Таким образом, традиционная экономика нуждается в серьёзной трансформации, что диктуется, с одной стороны, бурным развитием новых технологий, а с другой – неизбежностью отказа от устаревших догматов, где цель производства – максимизация прибыли, необоснованная погоня за прибылью. Потребуется радикальный пересмотр роли всех институтов, особенно государства.

Сегодня цифровая трансформация – это не только электронный документооборот, множество электронных сервисов и услуг, повсеместное применение цифровых помощников и т.п. Она затрагивает глубинные социально-экономические процессы, начиная от экономии транзакционных издержек и заканчивая вопросами занятости. В целом цифровая трансформация это прежде всего важнейшая предпосылка и мощный инструмент для построения новой низко затратной устойчивой экономики, свободной от социального неравенства, кризисов и негативного влияния на окружающую среду.

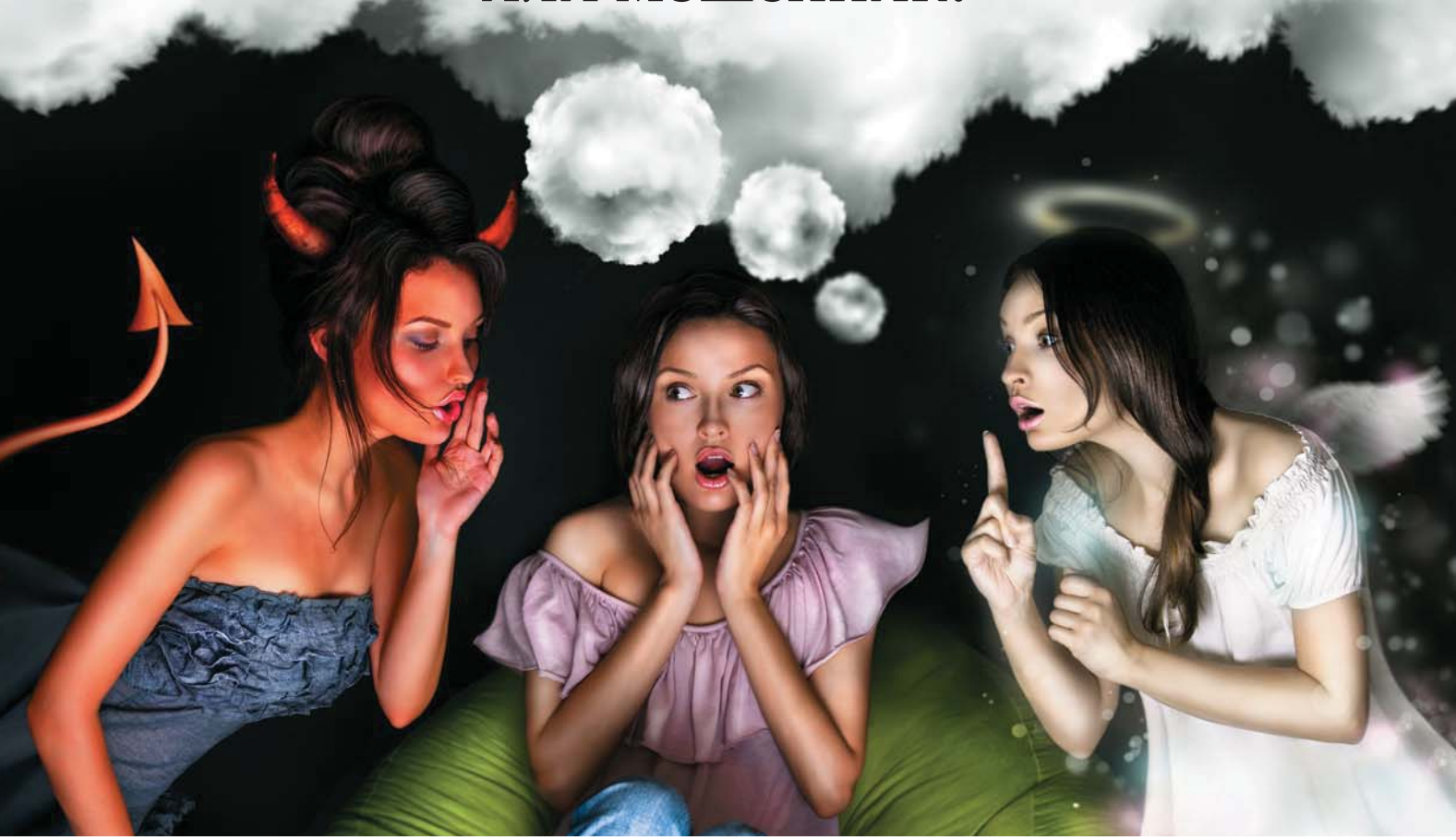
Такое построение можно осуществить в три этапа. Первый – совершенствование рыночных отношений. Второй – отказ от абсолютизации рынка. Третий – построение альтернативы существующей экономической модели.

Анатолий Орлюк
доцент МИИТа, к.э.н

8 985 215 18 36

an.orlyuk@yandex.ru

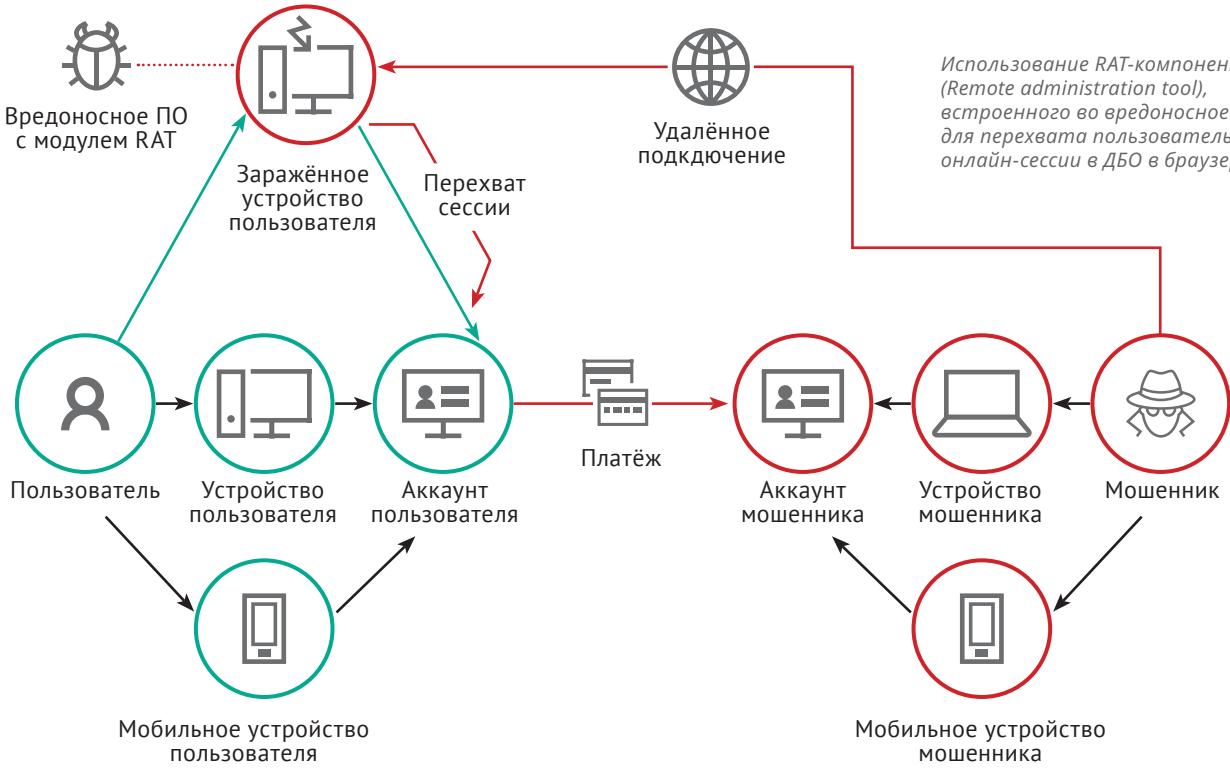
Как понять, кто пользуется вашим сервисом – реальный клиент или мошенник?



Растущий интерес бизнеса к переводу услуг в digital-пространство и онлайн-взаимодействию с клиентом оправдан. Сделав шаг в цифровизацию, компания получает множество выгод, включая экономию на операционных расходах и увеличение клиентской базы. Но такой переход открывает и новые возможности для кибермошенников...

Банки уже приучили нас как пользователей проводить большую часть операций через личные кабинеты интернет- и мобильного банкинга. Компании розничной торговли, медицинские учреждения, страховые компании и даже государственные структуры уже находятся в активной стадии цифровой трансформации. Выборы в государственные органы через интернет-голосование уже не кажутся чем-то фантастическим, и это подтверждают первые тестирования такого онлайн-подхода, прошедшие в Москве. И если в оффлайн-истории компания обычно взаимодействует с клиентом на физическом уровне, будь то магазин или отделение, то при использовании веб-сайта или мобильного приложения бизнес может опираться только на электронные признаки – имя пользователя, пол, частота использования сервиса, время, проведённое на сайте. Кроме того, перенос сервиса в онлайн открывает двери для кибермошенников, постоянно совершенствующих атаки как на устройство, так и на личный кабинет пользователя.

В случае кражи и использования мошенником учётной записи реального пользователя компания подвергается риску прямых убытков при краже денежных средств, накоплений или персональных данных пользователя из личного кабинета, ущербу репутации при утечке инцидента в СМИ и социальные сети, снижению доверия легитимных пользователей. Помимо компрометации учётной записи, мошенники могут просто «нагенерировать» новые учётные записи и привязать их к разным почтовым адресам, а иногда и к одному. Например, в конце 2017 года командой фрод-аналитики «Лаборатории Касперского» была выявлена группа из более 3000 синтетических аккаунтов, используемых для получения приветственных бонусов за новую регистрацию кабинета, и для управления всей группой аккаунтов использовался один почтовый ящик. Наличие большого количества синтетически созданных (фейковых) аккаунтов мешает точной оценке объёмов закупки товаров у поставщиков (особенно в дни сезонных распродаж), планированию логистической цепочки, препятствует органическому развитию программы лояльности.



Для финансовых организаций борьба с мошенничеством на электронных сервисах дополнительно ко всему регулируется ещё и на законодательном уровне, в том числе и в разрезе противодействия мошенничеству по части отмывания денежных средств через банки без ведома последних (115-ФЗ, 167-ФЗ, 382-П, 375-П).

Текущие методы проверки пользователя и почему они не работают

Задача специалистов информационной безопасности – усилить (или хотя бы сохранить) уровень безопасности, при этом не нарушив бизнес-процессы пользовательских сценариев сервиса. Текущие методы идентификации пользователя пока требуют от конечного пользователя дополнительных действий на входе в сервис и на этапе подтверждения какой-либо транзакции (например, перевод денег). Мы говорим о кодах в СМС, виртуальных и программно-аппаратных токенах, captcha, секретных вопросах. Такой подход усложняет покупательский путь до оформления заказа и проведения платежа. Более того, злоумышленники знают пути обхода таких проверок. Система Kaspersky Fraud Prevention фиксировала случаи, когда мошенник подключался к легитимной онлайн-сессии юридического лица, подтверждённого токеном, используя «троян» и средство удалённого управления (см. рис 1). И дело далеко не в слабой защите.

Киберпреступники регулярно совершенствуют методы обхода защитных средств. Поэтому специалисты информационной безопасности постоянно смотрят в сторону новых технологий и подходов от вендоров в области киберзащиты.

Технологии на основе машинного обучения – подход «нового поколения»

Решение «Лаборатории Касперского» Kaspersky Fraud Prevention выводит обнаружение мошеннической активности на новый уровень, позволяя реагировать на действия пользователя на ранней стадии, ещё до проведения транзакции, и помогая отличить легитимного пользователя от мошенника. Для повышения эффективности и точности обнаружения технологий применяются различные методы машинного обучения: кластеризация, деревья решений, нейронные сети. Система анализирует множество обезличенных параметров пользователя: характеристики устройства и его окружения, геолокацию, поведенческие шаблоны и пассивную биометрию, наличие вредоносных компонентов, ботов на устройстве и других атак – и создаёт профиль доверенного пользователя. В случае выявления какой-либо подозрительной и нетипичной активности в режиме реального времени Kaspersky Fraud Prevention мгновенно оповещает систему компании о риске мошенничества.

Ключевые преимущества

- Обнаружение сложных схем мошенничества: кражи учётной записи, синтетических аккаунтов, отмывание денежных средств – до проведения транзакции в режиме реального времени.
- Кросс-канальное обнаружение фрода – в веб- и мобильном сервисе
- Улучшение удобства использования сервиса для клиентов.
- Сокращение затрат на второй фактор аутентификации для доверенных пользователей (до 87%).

Глобальное присутствие «Лаборатории Касперского» позволяет легко идентифицировать «хорошие» устройства и использовать эти данные для аутентификации пользователя. По сути, «отпечаток устройства» выступает как дополнительный фактор аутентификации, так называемой Аутентификации на основе рисков (RBA или Risk-Based Authentication). Внедрив систему сессионного антифрода, бизнес усиливает безопасность своего сервиса и может предоставлять лучший пользовательский опыт своим клиентам в виде быстрого и лёгкого доступа к личному кабинету.

Екатерина Данилова
Менеджер по развитию бизнеса
Kaspersky Fraud Prevention

kaspersky

«Лаборатория Касперского» *– международная компания, работающая в сфере информационной безопасности.*
www.kaspersky.com | kfp.kaspersky.com/ru

Работаем из дома?

В последнее время широко распространена работа сотрудников из дома. Кроме того, наблюдается частое использование домашних компьютеров (ноутбуков) на работе. И в определённой степени это становится проблемой для организации. С одной стороны, сотрудник использует домашний ПК, а с другой – отсутствует гарантия, что этот ПК соответствует политике безопасности компании, в которой он работает.

Ещё большее количество угроз несёт этот вопрос в связи с развитием облачных технологий. Ведь где гарантия, что дома у вашего сотрудника используется лицензионное ПО, установлены и вовремя обновляются операционная система, антивирус, средства защиты и тем более ПО третьих производителей? Где гарантия, что подрастающее поколение не занесло «троян» под видом каких-то «улучшений» для прохождения игр? Вопросов гораздо больше, чем ответов.

На самом деле вариантов ответа несколько:

1. **Компания покупает и выдаёт сотруднику ноутбук для работы из дома.** Вариант наиболее дорогой, но предполагается, что корпоративный системный администратор всегда может управлять этим ПК, не беспокоясь о том, что сотрудник может что-то установить либо изменить в настройках. Потому что при таком подходе прав администратора у сотрудника быть не должно. Это затратное решение, но, с другой стороны, самый правильный выход из положения.
   Примечание. К сожалению, даже такой вариант не безгрешен. Ахиллесова пята заключается в редкой необходимости менять параметры в BIOS или загружать ноутбук в режиме восстановления, например при восстановлении штатной операционной системы при сбое. Как вариант, в этом случае пользователь должен сдать свой ноутбук и получить другой.
2. **Сотрудник работает с домашнего ПК, за который сам и отвечает.** Наиболее дешёвый, но самый рискованный вариант. Ведь фактически безопасность домашнего ПК никто не контролирует! Ну и что, зато бесплатно, – скажет недалёкий руководитель. Бесплатно ли? Не знаю, не знаю. Ведь в случае проникновения «вредоноса» с домашнего ПК сотрудника отвечать придётся всё равно вам – руководителю или системному администратору. А ваши пользователи умеют настраивать свой компьютер? Вовремя ставят обновления? У них всё программное обеспечение лицензионное? Да ну! И игры тоже? И фильмы они смотрят не с пиратских сайтов и торрентов? НЕ ВЕРЮ!
3. И последний вариант, который мне нравится больше всего, – **использование технологии Windows To Go.** В этом случае вы фактически покупаете только USB-флешку или SSD (что, на мой взгляд, куда предпочтительнее, хотя вроде и дороже). На самом деле, дороже, если не смотреть на срок службы. Да, вы можете купить сотруднику и внешний жёсткий диск. Единственное пожелание – покупать его под интерфейс USB 3.0, так он будет работать куда быстрее!

Впервые технология Windows To Go появилась ещё в Windows 8. Для создания соответствующего диска использовался образ корпоративной версии Windows. Причём создать можно было как с помощью мастера (в корпоративной версии), так и руками (в версии Pro).

Бывает, что вам нужно поработать на чужом компьютере, но сделать это так, как будто вы работаете на своём! То есть сделать так, чтобы от вашей работы не осталось бы ни следа. Да-да, любому специалисту покажется, что вас на этом компьютере вообще не было!

Идеальным выходом в этом случае будет режим Windows To Go. Ведь в таком варианте операционная система Windows будет установлена непосредственно на флешку! Однако стоит учесть, что загрузочный диск вы должны подключить непосредственно к USB-порту, то есть подключение через USB-хаб работать не будет!

Естественно, ёмкость вашего флеш-накопителя должна быть не менее 32Гб, но сегодня это не проблема. Учтите, что в ходе первой загрузки на конкретном ПК вам потребуется установить все драйвера для него, поэтому загрузка будет идти несколько дольше, чем в последующем.

Вместе с тем вам придётся вспомнить, что по аналогии с работой Windows To Go, созданной под управлением Windows 8, вам будут недоступны некоторые стандартные возможности:

4. После загрузки в режиме Windows To Go вам станет недоступен жёсткий диск, так как он будет находиться в состоянии off-line.
5. При использовании шифрования BitLocker следует учесть, что Trusted Platform Module (TPM) не используется.
6. Режим гибернации отключён, и понятно почему.

Естественно, среда восстановления Windows недоступна.

Кроме того, в Windows 10, в отличие от Windows 8, создание USB-носителя для Windows To Go теперь доступно не только версии операционной системы Windows 10 Корпоративная, которая, кстати, отдельно уже не выпускается, но и в версии Windows 10 Pro. Поэтому создавать USB-диск с Windows To Go вручную, как это можно было сделать на компьютере под управлением Windows 8 Professional, по-прежнему можно, но смысла не имеет!

Мало того, создавать такой USB-носитель вручную, используя только Windows 10 Pro, можно, но в результате получим USB-носитель,

Владимир Безмалый
Microsoft Security Trusted Advisor
Консультант ООН по вопросам информационной безопасности

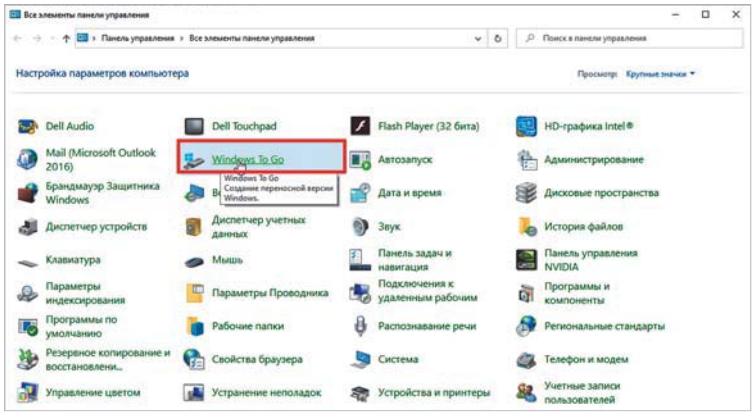


Рисунок 1. Панель управления.

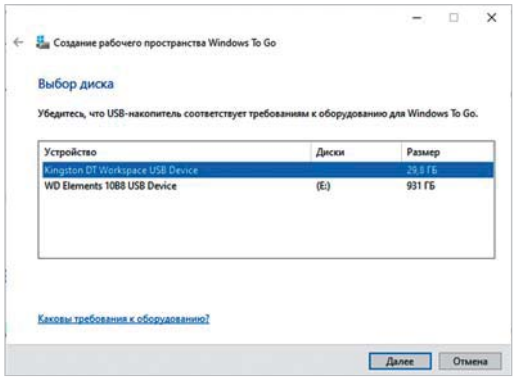


Рисунок 2. Выбор носителя.

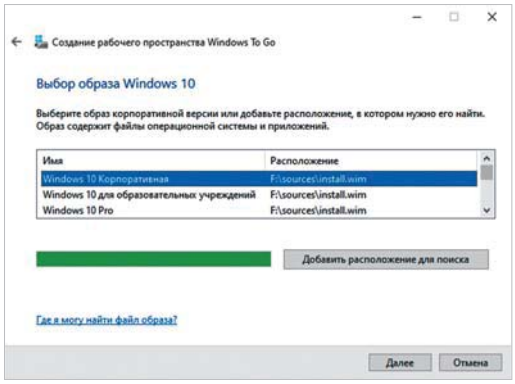


Рисунок 3. Выбор образа для Windows 10.

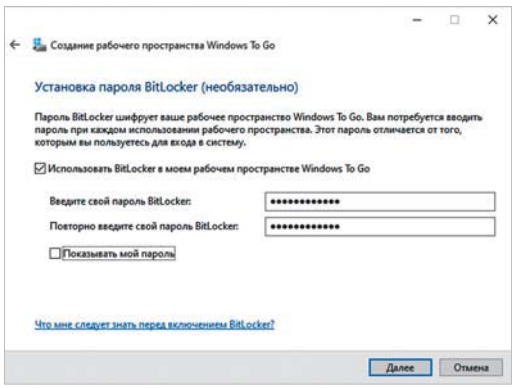


Рисунок 4. Установка BitLocker.

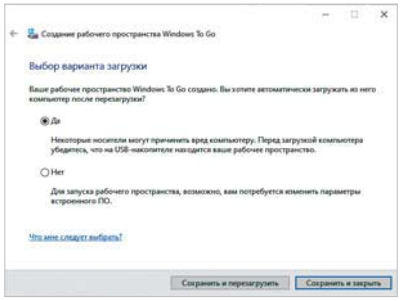


Рисунок 5. Окончание настройки

под управлением которого ваши локальные диски будут полностью видны. В некоторых ситуациях это весьма полезно, но не в случае работы в корпоративной сети из дома.

Создание носителя для Windows To Go с помощью мастера в Windows 10

Для создания диска Windows To Go вы должны войти в Панель управления. Выбрать режим отображения Крупные или Мелкие значки, а затем выбрать Windows To Go (рис. 1). После этого выберите носитель, на котором вы будете создавать Windows To Go (рис. 2). Смонтируйте Business версию ISO-файла Windows 10 и укажите этот образ как рабочее пространство, откуда будут скопированы необходимые файлы (рис. 3).

Если администратор при создании Windows To Go захочет зашифровать носитель с помощью BitLocker, то он может сразу это сделать. Учтите: так как TPM при этом недоступен, то потребуется просто дважды указать свой пароль шифрования. Помните: у вас нет возможности восстановления этого пароля.

Этот шаг является необязательным, но, если вы хотите, чтобы ваши сотрудники могли работать именно из дома, я считаю его обязательным. Ведь любой человек может потерять флешку, не так ли? А если она зашифрована, то весь ущерб от её потери равен стоимости флешки, что, в сущности, не так уж и много (рис. 4).

Не забудьте, что вы потеряете всю информацию, которая хранилась на вашем USB-носителе! Нажимаем «Создать», и ждём окончания процесса (рис. 5).

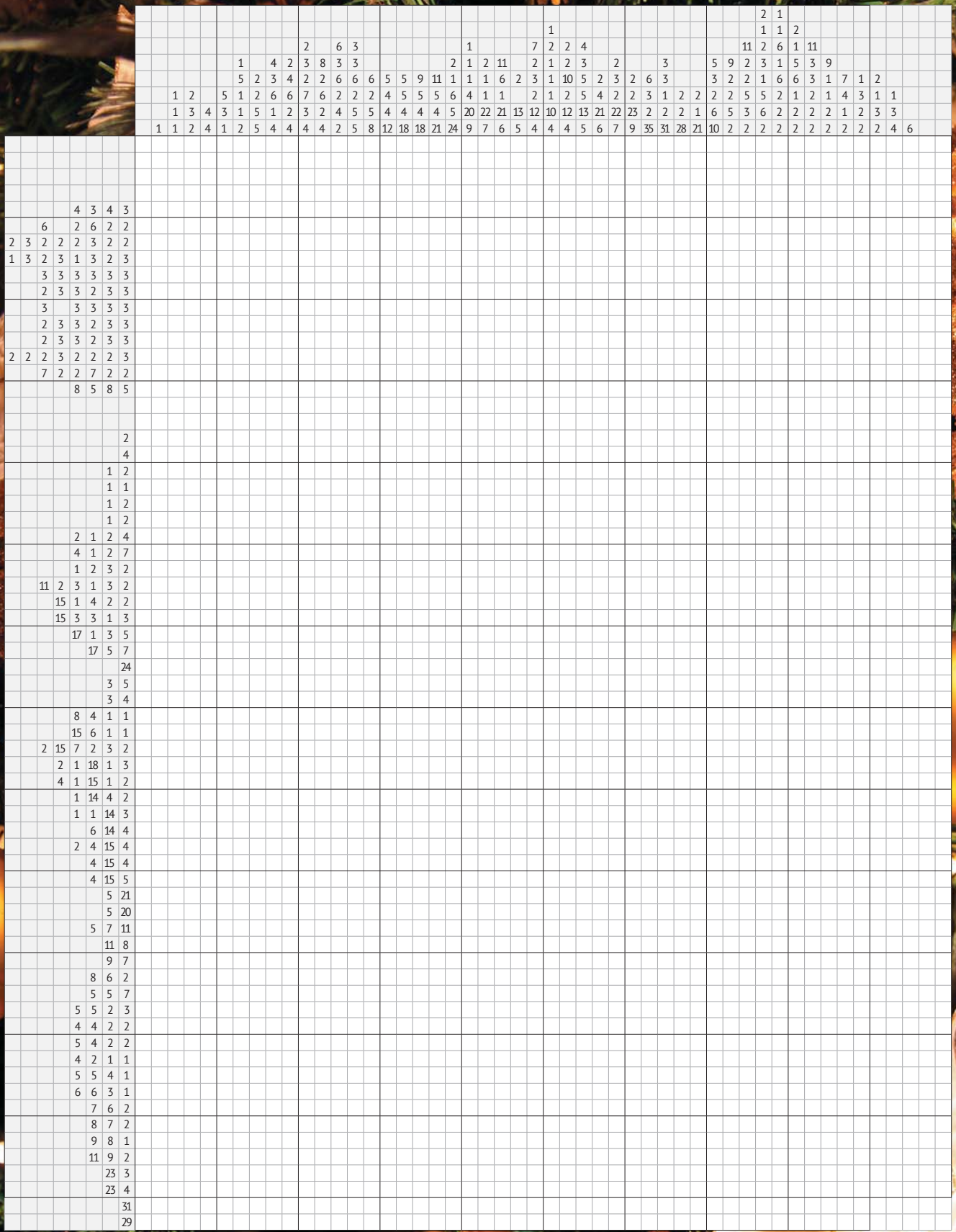
Таким образом, вместо того, чтобы морочить голову с настройкой домашнего ПК пользователя для доступа в корпоративную сеть, вы получаете зашифрованный носитель, который можно воткнуть в USB-порт и работать из дома или с любого другого «чужого» ПК. Не забудьте, что вы только что создали просто зашифрованный носитель с операционной системой. И не более. Для полноценной работы загрузитесь с такого носителя и установите на него нужное программное обеспечение, например: VPN, антивирус, удалённый доступ в вашу сеть и прочее.

Не забудьте убедиться, что ваш USB-носитель может быть загрузочным, иначе вся работа бессмысленна.

И ещё один совет. Ваш носитель должен обязательно поддерживать USB 3.0. В этом случае вы получите скорость работы не ниже, чем при работе с локального жёсткого диска, а возможно, и выше.

Согласитесь, такой вариант использования технологии существенно дешевле покупки нового ноутбука каждому, кому по тем или иным причинам потребуется работать из дома либо в командировке.

Японский кроссворд



Календарь мероприятий

28 ноября 2019
Онлайн-трансляция • Вебинар
Что ждет SEO в 2020 году?

28 ноября 2019
Санкт-Петербург • Лекция
Прокачай бизнес в онлайне! Практики и кейсы

28 ноября 2019
Новосибирск •Соревнование
II сезон QuizIT! Финальная игра

28 ноября 2019
Москва • Конференция
Преимущества рынка STO перед классическими венчурными инвестициями

28 ноября 2019-28 мая 2020
Онлайн-трансляция • Курс
Практический курс Middle Android Developer на Kotlin

29 ноября 2019
Москва • Конференция
Skolkovo LegalTech. Black Edition

29 ноября 2019
Москва • Конференция
RUSSIAN STARTUPS GO GLOBAL 2019

29 ноября 2019-2 декабря 2019
Москва • Хакатон
Хакатон Urban. Tech Moscow

29 ноября 2019
Уфа • Митап
PHP-митап в Уфе

30 ноября 2019
Уфа • Конференция
UFADEVCONF

30 ноября 2019
Москва • Онлайн-трансляция • Конференция
DataStart

30 ноября 2019
Москва • Турнир
Турнир по кикеру «IT»s KICKER Moscow 2019»

2-6 декабря 2019
Санкт-Петербург • Курс
Системный и бизнес анализ в разработке ПО. Интенсивный курс

5-6 декабря 2019
Москва • Онлайн-трансляция • Конференция
Heisenbug 2019 Moscow

7 декабря 2019
Москва • Конференция
DevOpsDays Moscow 2019

7 декабря 2019
Краснодар • Конференция
DevFest Krasnodar 2019: Back to The Future!

7-8 декабря 2019
Москва • Онлайн-трансляция • Конференция
Mobius 2019 Moscow

7 декабря 2019
Москва • Турнир
Турнир по боулингу «IT Strike Moscow 2019»

8 декабря 2019
Москва • Турнир
Турнир по шахматам «IT Chess Moscow 2019»

11-13 декабря 2019
Онлайн-трансляция • Курс
Поднимем сайт с колен: 3-дневный интенсив по продвижению

12-13 декабря 2019
Москва • Форум
Неделя Российского Интернета (RIW) 2019

12 декабря 2019
Минск • Конференция
Affiliate Marketing Conference Belarus

12 декабря 2019
Москва • Соревнование
Премия Рунета 2019

14 декабря 2019
Санкт-Петербург • Турнир
Турнир по боулингу «IT Strike St. Petersburg 2019»

16-19 декабря 2019
Москва • Курс
DPREP: Подготовка данных для Data Mining

15 января 2020-11 марта 2020
Санкт-Петербург • Курс
DevOps Engineer

24 января 2020
Москва • Конференция
Конференция о связи науки с современными технологиями Mieloconf

25 января 2020
Минск • Конференция
f (by) 2020

28 января 2020
Онлайн-трансляция • Мастер-класс
SEO-старт: основы продвижения

30 января 2020
Онлайн-трансляция • Мастер-класс
Самостоятельное SEO-продвижение

30-31 января 2020
Москва • Форум
Инфофорум-2020

Февраль 2020
Москва • Форум
Cyber Security Forum

3-5 февраля 2020
Москва • Конференция
PgConf. Russia 2020

4 февраля 2020
Онлайн-трансляция • Мастер-класс
SEO-продвижение интернет-магазинов

6 февраля 2020-6 марта 2020
Онлайн-трансляция • Курс
Самостоятельное продвижение сайтов «без воды»

17-21 февраля 2020
Республика Башкортостан • Форум
X Уральский форум Информационная безопасность финансовой сферы

19-20 февраля 2020
Москва • Форум
iFin

24 февраля 2020
Москва • Форум
Московский цифровой форум

Март 2020
Москва • Конференция
Код ИБ Профи

Март 2020
Москва • Конференция
IDC IT SECURITY ROADSHOW

18-20 марта 2020
Москва • Курс
BDAM: Большие данные Big Data для руководителей

Апрель 2020
Москва • Конференция
CISummIT

2 апреля 2020
Москва • Конференция
HotelCIO Exchange

3-4 апреля 2020
Москва • Курс
AIRF: Apache AirFlow

23-24 апреля 2020
Москва • Форум
CISO FORUM: взгляд в будущее

24-25 апреля 2020
Санкт-Петербург • Онлайн-трансляция • Конференция
HR API 2020

Май 2020
Москва • Форум
Positive Hack Days (PHDays)

5 июня 2020
Москва • Онлайн-трансляция • Конференция
Linux Moscow 2020

Сентябрь 2020
Москва • Конференция
Merlion IT Solutions Summit

15-17 сентября 2020
Санкт-Петербург • Форум
PKI – Форум

Октябрь 2020
Москва • Благотворительная ИТ-конференция
CISummIT «Digital Hearts»

Октябрь 2020
Москва, Сколково • Конференция
Russian Fintech Day

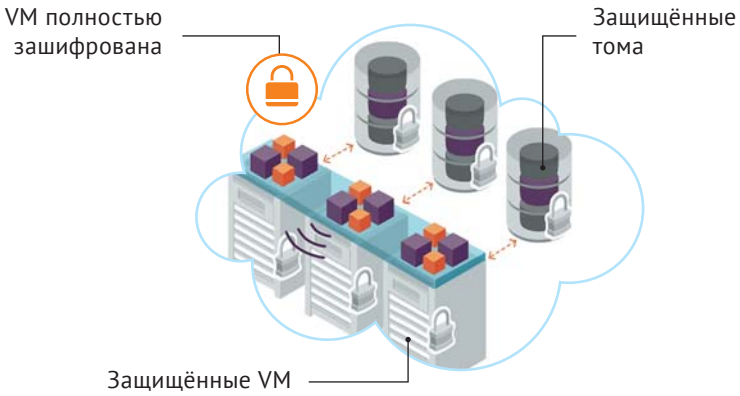
Ноябрь 2020
Москва • Конференция
Itsec

Ноябрь 2020
Москва • ИТ-конкурс красоты
Мисс CIS

ProtectV

Обеспечение полного шифрования VM

- **Шифрование всей VM**
  - Разделы с ОС
  - Разделы с данными
- **Шифрование всех связанных «снапшотов» и резервных копий (DR-сайты, и т. п.)**



Защита данных для виртуальной среды

ProtectV – промышленное решение по защите данных для виртуальной и облачной инфраструктуры. Решение обеспечивает:

- **изоляцию** данных
- **авторизованный запуск** VM
- **контроль доступа** ко всем копиям VM и дисков
- полную **блокировку** доступа в случае компрометации

ProtectV – возможность **безопасно** переносить важные элементы ИТ-инфраструктуры в «не доверенную» или общедоступную среду.

Поддерживаемые среды, продукты, производительность

- ProtectV сейчас поддерживает:
  - VMware vSphere
  - Microsoft HyperV
  - Amazon Web Services EC2
  - Amazon Web Services VPC
  - Microsoft Azure
  - IBM Bluemix
  - Google Cloud Platform
- ProtectV – влияние на производительность 5% – 10%
- Совместимые системы управления ключами шифрования:
  - SafeNet KeySecure (k250, k460, k450)
  - SafeNet Virtual KeySecure (k150v, k170v)

Читайте подробнее на стр. 22