ПЛЫВУЩИЕ ПО НЕБУ ОБЛАКА

Ермаш Артем Васильевич
ООО «Клауд Комьюнити»

2016 год наступил. Кажется, еще вчера мы спорили, когда правильнее праздновать миллениум и начало XXI века – в 2000 или в 2001 году. Незаметно из эпохи первой робкой поступи Интернета в России мы переместились в эпоху 4G-сетей, мобильных устройств, мощных ПК, очков дополненной реальности и… в холле нас встречает все тот же охранник, уныло переводящий взгляд с 17-дюймового монитора на 15-дюймовый телевизор.

Чуда не произошло – ни распознавания лиц, ни иной бесконтактной биометрии, все та же старая карта формата EM-Marine служит нашим пропуском для доступа в светлый кондиционированный офисный рай. XX век уверенно занимает все доступные ему ниши нашей жизни и не собирается их покидать – консерватизм в тренде.

Однако на этом фоне торжества консерватизма попробуем рассмотреть, не пропускаем ли мы что-нибудь из интересных новинок, теряющихся на фоне технологических колоссов образца конца XX века. И одна из тем, которая выступает за очертания колоссов, – централизованные информационные сервисы, появившиеся на волне мощного рывка технологий связи. Эти сервисы объединяют широким термином «Облачные технологии». Что нового свершившаяся информационная революция принесла в сферу систем безопасности?

ТРЕНДЫ И КОНТР-ТРЕНДЫ

Облачные сервисы на рубеже веков стали логическим продолжением тенденции на централизацию корпоративных вычислительных систем. Счастливые обладатели огромных распределенных парков вычислительных мощностей постепенно приходили в ужас от расходов на администрирование IT-инфраструктуры филиалов, растущих вслед за увеличением ее сложности. И в определенный момент всем стало понятно, что арендовать мощности в дата-центре дешевле, чем содержать локальную IT-инфраструктуру и бесчисленные отделы высококвалифицированных системных администраторов. А после того как был преодолен психологический барьер корпоративных управленцев, связанный с тем, что в удаленные дата-центры «уплыли» конфиденциальные данные, критически важные для работы их компаний, разработчикам IT-решений не составило труда убедить уже смирившихся с этим топ-менеджеров в передаче на аутсорсинг не только аппаратной части их IT-инфраструктуры, но и программных платформ и решений. Как только стали очевидны преимущества не только с точки зрения экономии затрат, но и надежности, эволюция IT-решений для бизнеса плавно и уверенно развернулась в сторону массового внедрения в секторе B2B облачных сервисов и услуг.

Однако плох тот специалист службы безопасности, который не страдает паранойей. А поскольку руководят службами безопасности хорошие сотрудники, то они заняли уверенную оборонительную позицию в отношении внедрения всевозможных централизованных решений. И для этого у них были весомые основания.

Во-первых, системы безопасности до сих пор довольно редко интегрируются с корпоративными системами управления (например, ERP – enterprise resource planning – системы управления производственными ресурсами; CRM – client resource management – управление работой с внешними контрагентами). И как следствие, упрощение доступа к данным систем безопасности удаленных филиалов за счет централизации – осязаемой операционной полезности для консервативного российского менеджмента предприятий не дает. В этой тенденции несомненно есть исключения – лидеры рынка в области связи, ритейла и некоторых производств уже используют системы контроля доступа и системы видеонаблюдения в комплексе со своими ERP/CRM системами, что позволяет менеджменту видеть производственные процессы под новым углом и дает менеджменту среднего уровня и работникам на местах новые возможности для работы с подчиненными и клиентами, но трендом эти решения пока не являются.

Во-вторых, важной составляющей интегрированных систем безопасности являются подсистемы охранного телевидения (СОТ), и пересылать по магистральным сетям гигабайты видеопотоков в централизованные хранилища – удовольствие не всегда реализуемое и недешевое даже в 2016 году.

А с учетом того, что пересылать нужно не только туда, но и обратно – это препятствие выглядит как непреодолимое.

Но не все так безнадежно, как может показаться на первый взгляд. Помощь в развитии облачных сервисов безопасности пришла с другой стороны – частные пользователи, гораздо менее искушенные, чем профессионалы, в вопросах конфиденциальности информации, уже в середине 2000-х начали формировать устойчивый спрос на решения, включающие возможность управления и мониторинга системами безопасности из глобальной сети. Как только на рынке появились недорогие IP-камеры для домашнего использования, пользователи начали самостоятельно решать вопросы доступа к ним через глобальную сеть. На первом этапе это были варианты с реальными IP-адресами для камер. И благо, что этот ресурс довольно быстро исчерпали, т. к. сочетание «белого IP» и сохранения настроек безопасности «по умолчанию» увели на просторы сети огромное количество home-video незадачливых пользователей. Все поняли, что доступ к частным ресурсам через реальные IP – это неправильно. В результате начали появляться сервисы, предоставляющие доступ к домашним видеокамерам через свои веб-интерфейсы и мобильные приложения за небольшую абонентскую плату – от 2 до 10 USD в месяц за камеру, с предоставлением облачного хранилища. Есть также бесплатные сервисы без возможности организации облачного хранилища.

Вторым фактором, задающим тренд, стали различные воплощения в жизнь концепции «Умного дома», которые делают жилище полноценным интерактивным устройством, с развитой логикой взаимодействия с человеком. А любое большое и дорогое интерактивное устройство для современного пользователя – это обязательный доступ к сервисным функциям через мобильное устройство, в т. ч. через глобальную сеть и мобильные сети, как частный случай. Да что там «Умный дом», современная автомобильная сигнализация уже умеет держать владельца «в курсе» всего происходящего и выполнять команды мобильного приложения.

И относительно недавно уже сами разработчики технических средств обеспечения безопасности начали предлагать пользователям различные инструменты, позволяющие получать информацию о состоянии систем и в определенных случаях управлять оборудованием на удаленных объектах. Вслед за решениями для сегментов охранных систем и «Умного дома», облачные сервисы для конечных пользователей начали предоставлять и разработчики систем видеонаблюдения – на сегодня все ведущие производители, представленные на российском рынке, имеют в своем активе такие предложения. Однако преимущественно это решения, по-прежнему ориентированные на запросы частного пользователя, желающего быть в курсе, как проводят время домашние его питомцы, посмотреть обстановку на паркинге своего автомобиля, а также иметь возможность дистанционно включить отопление на даче.

ОБЛАКА ИЛИ ОБЛАЧНЫЕ ЗАМКИ?

Вслед за частными пользователями, корпоративный сектор также начал формировать спрос на интегрированные платформы безопасности, позволяющие выстраивать распределенные и централизованные решения для предприятий с разветвленной структурой филиалов. Тон в развитии данного спектра решений в России стали задавать разработчики интегрированных платформ безопасности на базе систем видеонаблюдения. Все эти интеграционные платформы в своей архитектуре подразумевают построение именно сетевых распределенных решений с множеством серверов в едином интерфейсе.

Таким образом в сфере систем безопасности произошел переход от локальных решений к решениям с распределенной архитектурой. Однако, именно облачные сервисы в это время по-прежнему находились далеко за рамками мэйнстрима, хотя все разработчики интегрированных систем безопасности начали включать в пакеты предлагаемых решений веб-сервер для работы с системой через «тонкий клиент».

Здесь нам необходимо остановиться и уточнить, какое решение мы будем называть облачным сервисом и чем оно отличается от сервера интегрированной системы безопасности, размещенного в дата-центре оператора связи.

Облачный сервис – это в первую очередь изменение модели взаимодействия между производителем решения и его клиентами. Изменение заключается в продаже клиенту продукта или функционала (или какой-то его части) как сервиса, а не продаже лицензированных программно-аппаратных комплексов. Не могут считаться облачными сервисами функции, предоставляемые производителями решений бесплатно по модели «как есть», в комплекте с поставляемым оборудованием, и не создающие дополнительной прибавочной стоимости, которая оплачивается пользователями.

Нужно иметь в виду, что переход к работе по этой модели отнюдь не означает исчезновение из цепочки взаимодействия производителя решения и конечного пользователя такого важного звена, как системный интегратор, который по-прежнему занимается кастомизацией продукта и внедрением комплексного решения в соответствии с техническими требованиями конечного пользователя. Более того, с переходом к сервисной модели взаимодействия с заказчиком роль и значение квалификации системного интегратора только увеличивается.

Давайте рассмотрим этот аспект подробнее. При внедрении решения по классической модели параметризация требований к поставляемому комплексу происходит в рамках технических требований заказчика, которые формализуются в договоре на внедрение решения, ограничивающем собой юридически значимые обязательства между пользователем и интегратором. Обязательства сторон актуальны на время действия договора на установку и пуско-наладку решения, и частично – в течение срока гарантии. После завершения внедрения комплекс переходит в эксплуатацию специалистами заказчика, и качественные характеристики решения зависят от того, насколько корректно осуществляется эксплуатация комплекса. Деградация качественных характеристик внедренных решений – достаточно распространенное явление.

В отличие от классической модели, в сервисной модели взаимодействия все стороны непрерывно связаны между собой условиями SLA (service level agreement – соглашение об уровне сервиса). SLA детально фиксирует функциональные характеристики внедренного решения, а также регламентирует взаимодействие заказчика и исполнителя при обнаружении дефектов. Исполнитель при этом аналогичным образом связан с разработчиком решения. Это принципиально иной уровень взаимодействия, который образует сквозную ответственность всех сторон, участвующих в разработке, внедрении и эксплуатации решения, и подразумевает соответствующие требования к квалификации и организации работы системного интегратора и разработчика решения.

Однако бесплатного сыра не бывает. Обратной стороной сквозной ответственности разработчика и системного интегратора за качество предоставляемого решения и сервисов является стоимость услуг, которую конечный пользователь решения платит регулярно, в течение всего срока эксплуатации системы.

Другим важным свойством полноценного облачного сервиса является наличие для его пользователей возможности интегрировать в едином интерфейсе разные системы безопасности с разных объектов и, наоборот, делегировать доступ к имеющейся системе пользователям, находящимся вне информационного периметра объектовой системы безопасности. Это может быть необходимо в т. ч. при внедрении решения в рамках одной организации, когда управленческий персонал получает доступ к агрегированным данным систем безопасности без предоставления им доступа непосредственно к интерфейсам систем.

ЗАЧЕМ ВСЕ ЭТО ВЕЛИКОЛЕПИЕ?

Невзирая на привлекательность обертки в виде гарантированных характеристик работы внедряемых решений с элементами облачных сервисов, любой управляющий всегда внимательно будет смотреть на эксплуатационную стоимость решения. И как часто бывает, появление новой строки в операционных расходах (OPEX) на оплату сервиса, поставляемого 3-й стороной, вызывает у финансистов настойчивое желание ее удалить, вопреки утвержденному решению специалистов по эксплуатации инженерных систем (в том числе систем безопасности). В такой ситуации им необходимо проявить, с одной стороны, твердость в отстаивании принятого решения, с другой стороны, мудрость, которая позволит не войти в прямое противостояние с финансовыми управляющими.

Самый правильный способ избежать противодействия и попыток оптимизировать бюджеты проектов на внедрение информационно-технических систем – включить их в информационные системы предприятия (ERP/CRM) в качестве дополнительных источников данных. И здесь, несмотря на существенное развитие бизнес-аналитики в системах видеонаблюдения и контроля доступа, раскинулось огромное необработанное поле для развития. Именно облачные сервисы являются наиболее приспособленным интерфейсом для задач предоставления бизнес-пользователям дополнительной информации. Это и данные видеоаналитики, и данные для анализа производительности труда в рамках бизнес-процессов предприятия, которые позволяют наглядно подтвердить или опровергнуть информацию, предоставляемую менеджменту по управленческой вертикали. Наличие источника информации, не подверженного воздействию сознательного человеческого фактора, в некоторых ситуациях является единственным способом выявления дисбалансов в распределении сфер ответственности, производственных и трудовых ресурсов. Именно аналитика от систем безопасности может легко выявить нетипичные сценарии орг. процессов, например, в виде изменения графика активности персонала или клиентов в торговой точке, непредвиденного выхода ИТР на работу в выходной день или хронической переработки части бухгалтерского персонала одного из филиалов. Никакие совещания и поездки ревизоров такие аспекты работы компании выявить не позволят, пока эти отклонения не трансформируются в конфликтную или аварийную ситуацию, и известно это станет явочным порядком.

Конечно, учет и отслеживание производственных процессов с применением подобных инструментов – это удел крупных производственных предприятий, и на сегодняшний день в России небольшое число компаний ставит перед собой задачи по оптимизации производственных процессов на подобном уровне. Отчасти это связано с относительно простыми схемами организации бизнеса, доминирующими на российском рынке, отчасти с управленческими традициями, которые пока развиваются в русле модернизации советских производственных отношений с традиционной жесткостью вертикальных управленческих связей, не предназначенных для гибкого управления предприятиями. Однако, как показывает практика западных компаний, при достижении определенных масштабов деятельности, организация эффективных ERP и CRM систем обязательно сопряжена с получением дополнительной аналитики от систем безопасности и систем контроля доступа.

Для оценки тенденций, которые могут ожидать нас в ближайшем будущем, будет полезно посмотреть на требования к предлагаемым решениям западного корпоративного сектора на примере исследования, проведенного в США в 2014 году Eagle Eye Networks, Inc *http://www.eagleeyenetworks.com/cloud-video-surveillance-report-2014/*

В исследовании приняли участие 500 специалистов, которым были заданы вопросы об их профессиональной принадлежности и бизнес-планах по внедрению интегрированных систем безопасности.

Как видно из диаграммы, менеджмент, IT-специалисты и специалисты производства составляют более 2/3 заинтересованной аудитории в сфере систем безопасности. Это достаточно красноречивое свидетельство востребованности интеграционных решений для ERP/CRM систем предприятий.

Следующий вопрос был о том, как специалисты видят приоритетные задачи и что они планируют решить в рамках предстоящей модернизации или установки новой системы видеонаблюдения.

Здесь снова мы видим, что задачи операционного мониторинга бизнес-процессов предприятия актуальны более чем для 2/3 респондентов исследования.

Следующим вопросом было, какие конкретно аналитические и мониторинговые функции видеонаблюдения представляют интерес для участников исследования.

Как мы видим, лидируют функции, связанные с повышением качества обслуживания клиентов и повышением эффективности труда наемных работников – это отражает изменение в составе традиционных бизнес-пользователей систем видеонаблюдения и контроля доступа от специалистов служб безопасности в сторону менеджмента, специалистов по IT и руководителей производства.

Это изменение не могло не сказаться на отношении бизнес-пользователей к применению решений с облачной или комбинированной архитектурой. Вот как специалисты, планирующие внедрение систем видеонаблюдения, ответили на вопрос о предпочтительной архитектуре системы видеонаблюдения.

Мы снова видим характерное распределение в виде 2/3 потенциальных заказчиков решений, предпочитающих внедрять систему с возможностью рабо-

Диаграмма. Участники опроса

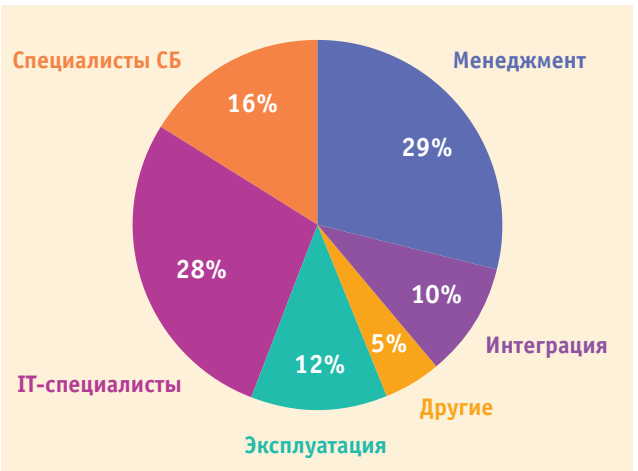

Диаграмма. Актуальные задачи

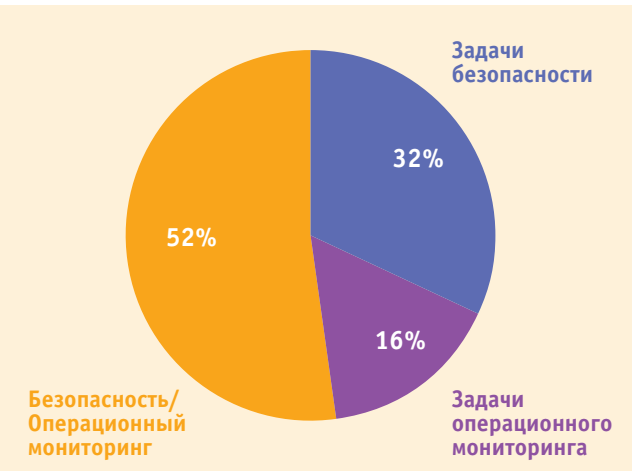

Диаграмма. Видеоаналитика: цели внедрения

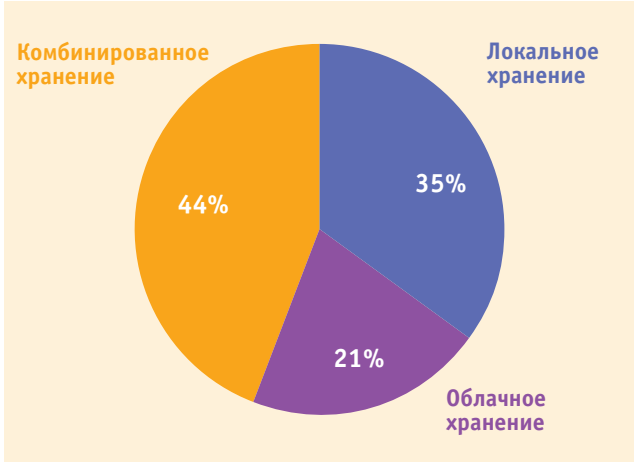

Диаграмма. Предпочтительная архитектура видеонаблюдения

ты с он-лайн и архивным видео через облачный сервис.

НЕЗАМЕТНАЯ ПОСТУПЬ НОВЫХ РЕШЕНИЙ

Исходя из представленных данных, мы можем констатировать смещение интереса к внедрению систем безопасности от специалистов СБ в сторону менеджмента предприятий, заинтересованного в повышение качества сервиса и производительности труда сотрудников. Соответственно, мы наблюдаем пропорциональный рост интереса во внедрении решений, позволяющих организовать легкий обмен данными, собираемыми с разных филиалов, с другими системами, а также имеющих возможности удобного доступа к информации при нахождении вне офиса.

В следующих частях нашего материала мы посмотрим, какие преимущества видят американские менеджеры в применении решений с элементами облачной архитектуры, а какие аспекты решений вызывают у них беспокойство. А также начнем знакомиться с примерами практического применения систем безопасности в разных отраслях деятельности.