


# Круглый стол:

## ИТ-подходы к рынку безопасности

Применение ИТ-решений в системах безопасности — это устойчивый тренд, который, с одной стороны, привлекает ИТ-компании на рынок ТСБ, а с другой — вынуждает традиционных безопасников становиться ИТ-интеграторами. Участники заочного круглого стола журнала RUBEЖ выяснили, насколько эти процессы затрагивают традиционные сегменты рынка безопасности — CCTV, СКУД, охранную и пожарную сигнализации, обсудили востребованность облачных технологий и дали прогноз на развитие ИТ в сегменте безопасности.

 Подготовила: Евгения Лысенко

### Участники круглого стола:

#### Александр Журавский,

технический директор,  
компания Iron Logic

#### Александр Коробков,

главный архитектор, компания Macroscop

#### Александр Крахмалев,

заместитель генерального директора,  
Группа компаний «Сигма-ИС»

#### Александр Макаров,

ведущий инженер, ЗАО «Риэлта»

#### Антон Садов,

старший технический специалист,  
ООО «Девлайн»

#### Вячеслав Тесаков,

генеральный директор,  
ООО «Равелин»

#### Александр Хегай,

заместитель руководителя отдела  
информационной безопасности,  
ООО «ЛАНИТ-Интеграция»

#### Максим Березин,

руководитель направления облачных  
технологий, директор Виртуального  
дата-центра «ПРОК»

### Что эффективнее при разработке систем безопасности — собственная команда или аутсорсеры?

#### Александр Журавский

Эффективность зависит от специфики применения. Например, контроллер отдавать на аутсорс не стал бы. Все-таки это критичный узел, поэтому хочется быть уверенным в компетентности разработчика. Кроме того, время диктует новые требования. И кто будет дорабатывать firmware? А вот разработка интерфейса пользователя, очевидно, будет эффективна на аутсорсе. А вообще ответ на вопрос зависит от того, что каждый для себя считает эффективным.

#### Антон Садов

По нашему опыту — собственные разработки. Наша компания старается идти по собственному пути развития, имея свой штат разработчиков. Иногда для решения каких-то узкоспециализированных задач наших клиентов или наших идей мы прибегаем к помощи аутсорс-специалистов, но в основном наша система разрабатывается штатным слаженным коллективом, работающим уже более десяти лет. Специфике нашей деятельности нигде не обучают, так что можно сказать, что все фирмы, разрабатывающие программное

обеспечение для видеонаблюдения, проходят тернистый путь саморазвития. Опыт показал, что аутсорс эффективен и экономически целесообразен для кратковременных решений. Но, помимо внедрения чего-то нового, требуются последующая модернизация и поддержание решения в актуальном состоянии, а также возможность совместной работы всех систем в целом, что при привлечении аутсорс-специалистов не всегда актуально.

#### Александр Крахмалев

Эффективнее для чего? Эффективность для организации — это получение большей прибыли. Эффективность для системы безопасности, как и качество самой системы, зависит от качества предлагаемых товаров и услуг. Собственные разработки значительно сложнее продвигать на рынок. Для успешной работы на рынке они и аутсорсинг должны дополнять друг друга.

#### Александр Макаров

Когда с нуля разрабатывается даже самый простой извещатель, найти необходимых специалистов на аутсорсе не так просто.

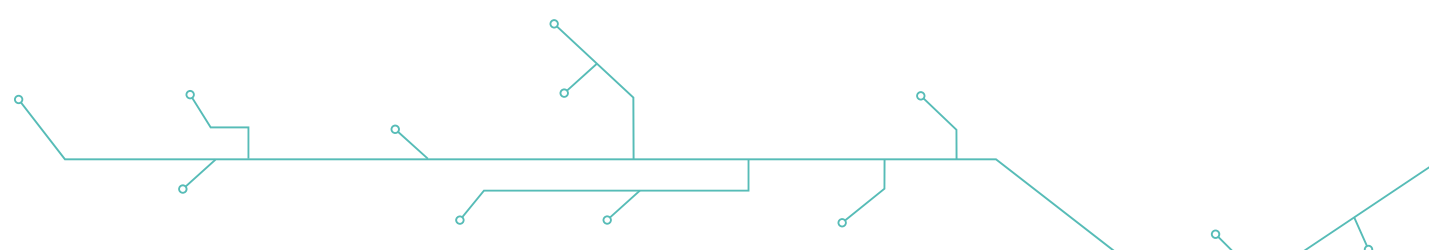
В извещателе сходятся и физические процессы обнаружения, и математическая обработка, и конструктивные требования, а также необходимость проведения полного комплекса испытаний. Найти такого специалиста на стороне практически невозможно.

#### Вячеслав Тесаков

Разработка подобной системы требует высокой компетенции от специалистов, следовательно, является крайне дорогой при производстве. Разработку собственной системы могут себе позволить только очень крупные компании или корпорации. Для всех остальных оптимальным путем является привлечение сторонних производителей, имеющих собственные наработанные решения.

#### Александр Хегай

Правильным решением будет являться сочетание этих подходов. В текущей рыночной ситуации с повышением валютных курсов спрос на отечественных разработчиков и перенос аутсорсинговых составляющих бизнеса в отечественные условия для многих станет крайне актуальным.



## Не секрет, что СБ компании с осторожностью относятся к облачным решениям. Насколько обоснованы опасения ваших заказчиков?

### Максим Березин

Замечу, что постепенно недоверие даже со стороны таких строгих заказчиков, как банки, уходит в прошлое. Облака уже фактически превратились в привычный рабочий инструмент, надежность и безопасность которого обеспечивается и задокументированными SLA, и отказоустойчивым оборудованием, и дополнительными средствами защиты, которые в том числе могут быть сертифицированы ФСТЭК и ФСБ. А чтобы быть полностью уверенными в безопасности систем, размещенных в облаке, мы в первую очередь рекомендуем обращаться к проверенным облачным провайдерам, которые эксплуатируют надежные дата-центры и имеют значительный опыт реализации облачных проектов.

### Александр Журавский

На мой взгляд, противоречия нет. Разумеется, доступ в какое-либо хранилище не следует организовывать на базе облачных технологий, а вот доступ к рабочему месту и учет рабочего времени — очень даже можно. Атаковать систему без получения материальной выгоды серьезные взломщики не станут. В случае облачного решения система контроля доступа иногда даже более защищена от действий злоумышленников внутри компании, чем локальная. Ну и для тех, кто совсем ничему не верит, наши устройства снабжены переключателем, блокирующим изменение баз в контроллерах извне. То есть провел изменения, заблокировал их переключателем — и не нужно опасаться взлома, тем более можно всегда восстановить резервную копию.

### Александр Коробков

Главным сдерживающим фактором перехода к облачным технологиям являются повышенные риски, связанные с безопасностью и приватностью. Такого рода опасения имеют место быть, но это справедливо не только для сферы видеонаблюдения, а для любых облачных сервисов. При этом ежедневно миллионы людей пользуются, например, электронной почтой и не опасаются передавать конфиденциальные данные. Операторы облачных сервисов видеонаблюдения в первую очередь за-

интересованы в обеспечении безопасной передачи и надежном хранении видеоданных, ведь это гарант их репутации. Поэтому для обеспечения надежности применяются различные технологии защиты: шифрование информации при передаче, разграничение прав доступа для пользователей при просмотре, резервирование и репликация при хранении.

### Александр Крахмалев

Должно существовать разделение объектов на классы по уровню важности и опасности. На объектах определенного класса облачные технологии должны быть полностью исключены. Для задач вроде охраны квартир, частных автомобилей и т.д. облачные технологии вполне уместны и эффективны. Однако и в этом случае также нужно учитывать специфику систем безопасности, прежде всего надежность и защищенность.

### Александр Макаров

Думаю, для этих опасений есть основание. Проблема состоит в необходимости обеспечения безотказного, резервированного и защищенного канала связи. Повсеместно в системах безопасности внедряются решения с двумя независимыми каналами связи. По одному из этих каналов данные вполне могут передаваться в облако.

### Антон Садов

Данный вопрос тревожит службы безопасности не без основания. Крупные компании стремятся реализовать определенный функционал за счет своих средств, через свои каналы связи, чтобы обеспечить доступ только определенному кругу лиц. Для безопасности это правильное решение, но реалии рынка, технический прогресс и финансовая составляющая данного вопроса не всем позволяют строить свои ЦОД, отдельные защищенные КСПД, иметь штат квалифицированных специалистов по обслуживанию всей структуры. На помощь приходят решения именно облачного взаимодействия, на которые, между прочим, есть спрос. Направление развивается, фирмы, предоставляющие подобные сервисы, также не стоят на месте, улучшают меха-

низмы защиты и отказоустойчивости систем, причем этот показатель может быть даже выше и лучше по сравнению с локальной системой хранения данных. Считаю, что для рынка систем безопасности должен быть выбор решений под конкретные задачи и условия.

### Вячеслав Тесаков

Если компания действительно созрела для использования облачных технологий — и то есть обладает разветвленной структурой и территориально разбита — она должна создавать свое частное облако, при этом ответственно подходить к выбору обслуживающей компании. Нельзя полностью доверяться облачным технологиям, надеясь, что из облака ничто и никогда не пропадет.

### Александр Хегай

Наш опыт показывает, что опасения служб безопасности по отношению к облачным технологиям можно условно разделить на два типа: опасения за свои данные в зарубежных облаках и в отечественных. Что касается обработки своей информации в отечественных облаках, то этот рынок в России еще только начинает развиваться, большинство компаний уже имеет собственную развитую инфраструктуру, перенос которой в облако без возможности остановки текущей деятельности и текущих бизнес-процессов в некоторых случаях может быть невыгоден. Так что такие опасения больше связаны с финансовыми показателями, нежели с угрозами несанкционированного доступа и регуляторными вопросами. Что касается зарубежных облаков, то в зависимости от данных, которые передаются туда на обработку, они могут нести в себе регуляторные риски, а также, в связи с текущей политической обстановкой, существенные риски несанкционированного доступа к данным или же приостановки бизнес-процессов, с ними связанных. Зарубежная облачная проблема может быть решена путем стабилизации экономическо-политической ситуации, а также более детального законодательного регулирования процессов обработки данных за рубежом.

## Какую роль вы отводите облачным решениям?

### Максим Березин

Облачные технологии — это одно из наиболее перспективных направлений в «КРОК». Оно ежегодно динамично растет. Так, по итогам 2015 года выручка от облаков в структуре бизнеса нашей компании увеличилась на 50%, а количество заказчиков возросло на треть. В перспективе мы рассчитываем на не менее активное развитие, которому будет способствовать рост доверия к технологии, ее зрелость, а также вступление в силу новых законодательных инициатив. В частности, поправки в закон о персональных данных подхлестнут увеличение облачного сегмента, так как именно облака позволят быстрее перенести персональные данные на территорию России без изменения архитектур ИТ-систем.

### Александр Журавский

Мы считаем, что облачные решения имеют большую перспективу. Стремительное развитие сетей, повышение их пропускной способности и снижение цены канала связи уже создали нишу для этой технологии. А возможность бесконечно масштабировать при отсутствии каких-либо сложностей с монтажом или настройкой VPN значительно повышает надежность и снижает требования к обслуживаемому персоналу. Наша компания считает это направление перспективным и динамически развивающимся.

### Александр Коробков

Уже не первый год на ИТ-рынке наблюдается тенденция переноса софта в облако: Gmail, Skype, Evernote, «Яндекс.Диск» — лишь небольшая часть облачных сервисов, которыми ежедневно пользуются миллионы людей. Вполне закономерным является перенос этой тенденции на рынок охранного видеонаблюдения и переход от традиционных систем к облачным. По данным компании M&M (MarketsandMarkets), мировой рынок VSaaS растет с темпом 30% в год. Рост популярности обусловлен простотой развертывания сервиса, отсутствием первоначального вложения капитала в инфраструктуру. Сейчас наша компания наряду с ПО для построения не облачных видеосистем разрабатывает Macroscop Cloud — программный комплекс для организации сервисов видеонаблюдения как услуги (VSaaS), позволяющий телекоммуникационным операторам подключить неограниченное количество камер и абонентов к облаку.

### Александр Макаров

В системах ОПС облачные решения развиваются достаточно активно, но большинство

выпускаемой нами продукции используется для передачи информации внутри одного объекта. В таких решениях применение облачных технологий не требуется. Кроме того, системы безопасности должны обладать высокой степенью надежности работы и не зависеть от сторонних сервисов, что ограничивает применение облачных технологий в системах безопасности.

### Антон Садов

Облачные решения — интересная идея с большой перспективой, нами они активно применяются с 2014 года. У нас есть два сервиса по данному направлению: «Аренда облачного сервера» предлагает в аренду выделенные серверы, находящиеся в дата-центре с предустановленной системой видеонаблюдения «Линия». Они полностью заменяют функционал стационарных IP-видеосерверов «Линия» на объектах. Клиент предоставляет только свои IP-камеры, доступные в Интернете, и может пользоваться данным сервисом как на постоянной основе, так и для возможности обеспечения надежности хранения информации. «Линия Облако» — это онлайн-сервис, предоставляющий пользователю инструменты для контроля состояния всех имеющихся серверов. Упрощает работу и контроль состояния серверов, дополнительно расширяет возможности программного обеспечения. Также на базе этого сервиса нами разрабатываются и внедряются дополнительные возможности.

### Вячеслав Тесаков

Направлением облачных технологий мы постоянно интересуемся. В системах безопасности облачные технологии применимы в основном в корпоративных решениях. Например, удобно размещать в облаке учет рабочего времени.

### Александр Хегай

Облачные технологии становятся все более популярными. Что касается переноса существующей инфраструктуры в облако, то у наших клиентов есть некоторые финансовые опасения по этому поводу, так как для крупных компаний это связано с проблемой значительных капитальных затрат и приостановкой бизнес-процессов. Если говорить об аспекте информационной безопасности, то здесь возникают вопросы несанкционированного доступа к данным, а также законодательного регулирования ответственности за несоблюдение процессов обработки информации конфиденциального характера.



## Назовите три основных ИТ-тренда на рынке безопасности

### Александр Журавский

Основными трендами являются защита от копирования меток, облачные технологии и более тесная интеграция с охранно-пожарными системами. Копирование меток — сейчас большое место в системах контроля доступа. Мало кому понравится, когда на придомовую территорию через установленный шлагбаум начинают проезжать незнакомые личности. Не секрет, что для копирования радиобрелока необязательно брать его в руки, достаточно «подслушать» передачу — и можно сделать копию. Все потому, что система не использует все возможности, предоставляемые чипом брелока. То же касается бесконтактных и контактных идентификаторов, которые копируют на каждом углу. Современная система должна быть защищена от подобных посягательств. Наша компания предлагает ряд решений по защите от копирования идентификаторов.

### Александр Крахмалев

Тренды — это то, что на нас сейчас движется, но не могу сказать, что это очень хорошо, в каждом есть перспективы, но и множество подводных камней и проблем, которые нужно учитывать.

Могу отметить следующее:

1. Новые каналы передачи данных, их доступность, в том числе и экономическая.
2. Скорость, большая пропускная способность (что важно прежде всего для СОР), надежность и возможность защиты информации в новых информационных каналах.
3. Переход всех систем безопасности (СОТ, СКУД и даже ОПС) на IP-интерфейсы.

### Вячеслав Тесаков

Первый тренд — это интеграция различных систем безопасности и других программ в одну. Второй — защищенность. Особенно это касается IP-систем. Наконец, востребованы сейчас и беспроводные системы. Здесь нужно подчеркнуть важность надежных линий связи и источников питания.

### Александр Коробков

В сфере видеонаблюдения я бы выделил следующие тренды:

1. Переход от ПО к готовым программно-аппаратным решениям (сетевым видеорегистраторам NVR). В мире наблюдается все возрастающая потребность в законченных программно-аппаратных решениях. В частности, пользователи и installеры предпочитают купить готовый продукт — видеорегистратор NVR, нежели по отдельности приобретать оборудование и ПО, а затем устанавливать и настраивать его.

2. Повышение значимости технологий искусственного интеллекта, и в частности компьютерного зрения, например в функциях видеоанализа, на который активно растет спрос. Системы видеонаблюдения постепенно перестают быть средствами получения, записи и отображения видео, а все больше включают в себя функции аналитики, помогающие оперативно принимать решения в режиме реального времени, а также быстро восстанавливать картину происшествий по видеоархиву.

3. Повышение степени сжатия (H.265). Повышение разрешения IP-камер пропорционально повышает требования к пропускной способности сети и размеру хранилищ видеоархивов. В силу того, что разрешение и объемы передаваемого видео растут быстрее скорости передачи по сети, большее значение играет степень сжатия видео. Потребность в более высокой степени сжатия привела к появлению в 2013 году нового стандарта сжатия H.265, позволяющего вдвое уменьшить размер видео по сравнению с H.264.

В 2014 году у различных производителей стали появляться первые IP-камеры с поддержкой H.265. На текущий момент уровень его распространения еще невысок, вследствие чего производители ПО и NVR не спешат добавлять его поддержку. Тем не менее из опыта внедрения H.264 можно сказать, что примерно через два года H.265 постепенно начнет вытеснять H.264. Наряду с этими трендами сохраняется тренд перехода к модели VSaaS (Video Surveillance as a Service).

### Александр Макаров

1. Переход к системам с повышенной информативностью.
2. Резервирование каналов передачи информации.
3. Интеграция различных систем на разных уровнях.

### Антон Садов

1. Беспроводные средства передачи информации.
2. Мобильность и компактность.
3. Многофункциональность — решения обрастают дополнительными возможностями, помимо основной своей направленности.

### Александр Хегай

Текущими основными трендами информационных технологий в сфере технических средств безопасности являются защита облачных инфраструктур, защита от угроз нулевого дня и средства комплексной аналитики информационной безопасности.

**Возможна ли на рынке безопасности замена локальных решений облачными с целью снижения издержек?**

**Максим Березин**

Да, и как наиболее яркий пример этого — использование гибридных облаков при тестировании и разработке нового функционала ИТ-систем при обучении персонала. Одним словом, при любых задачах, возникающих периодически и требующих резкого увеличения вычислительной мощности. Кроме того, способом оптимизации затрат может стать размещение в облаке ИТ- и бизнес-систем, нагрузка на которые носит сезонный характер. Например, интернет-магазинов, интерес к которым увеличивается в период распродаж и праздников. За счет гибкости распределения платежей в зависимости от потребления также проще управлять затратами на ПО. И еще один фактор экономии — сокращение сроков развертывания новых сервисов за счет отказа от закупки, инсталляции, настройки оборудования. Для многих компаний время — это по-прежнему деньги.

**Александр Журавский**

К этому все и идет. Так, например, ежемесячная плата за два контроллера и 200 карточек в облачном решении GuardSaas ниже платы за электричество, потребляемое локальным сервером. А если добавить человека, который должен делать резервные копии и обеспечивать восстановление компьютера после очередного отключения электри-

чества, то экономический эффект должен покрыть все страхи и опасения.

**Александр Коробков**

Я уверен, что это возможно. Более того, экономическая выгода — это один из факторов перехода к облачным системам. Пользователь избавлен от стартовых инвестиций для построения системы, а совместное использование ресурсов одного оператора многими пользователями снижает удельную цену на оборудование и обслуживание в расчете на одного пользователя.

**Александр Макаров**

Использование облачных сервисов с целью снижения издержек рационально только при построении крупных, масштабируемых, территориально разделенных систем. Такая замена в будущем возможна при соблюдении условий обеспечения надежности, безопасности и резервирования передаваемых данных.

**Антон Садов**

Трудно ответить однозначно. С одной стороны, какие-то решения позволяют снизить затраты на обслуживание, покупку и поставку на баланс предприятия. С другой стороны, если рассматривать по времени эксплуатации, то аренда выходит дороже локальной системы. Можно с уверенностью сказать, что

облачные сервисы дают дополнительные возможности. Например, если брать наш сервис аренды облачного сервера, то он позволяет начинающему предпринимателю или стартап-компания сэкономить деньги в начале, а клиенту, у которого уже используется локальная система видеонаблюдения, — обеспечить дополнительную сохранность данных. Соответственно, издержки на обеспечение безопасности в целом увеличатся, но, как известно, информация бесценна, каждый для себя сам определяет цену вопроса.

**Вячеслав Тесаков**

Можно говорить о снижении издержек только применительно к крупным компаниям. Сначала нужно перерасти локальные решения, чтобы перейти на облачные. То есть это вопрос развития бизнеса.

**Александр Хегай**

В случае изначального выбора облачных решений можно будет значительно снизить капитальные расходы, в случае миграции с существующей инфраструктуры и средств безопасности необходимо будет учесть высокие капитальные расходы на сам процесс перехода. В любом случае основой для принятия решения об использовании локальных или облачных решений безопасности должен являться глубокий анализ выгод и затрат.

**Какова специфика создания программных продуктов для систем безопасности по сравнению с другими сегментами, например CRM?**

**Александр Журавский**

Специфика заключается в том, что с программным обеспечением для СКУД непосредственно взаимодействует ограниченный круг людей. В ряде случаев взаимодействие носит эпизодический характер — ежемесячный отчет о посещении или необходимость добавить нового сотрудника. Хотя в больших фирмах, где есть служба охраны, взаимодействие с ПО уже постоянное, но тем не менее также ограниченного круга людей. Из всего этого следует, что чем более интуитивно понятны интерфейсы и защита от неправильных действий, тем больше будет положительных отзывов и меньше звонков в техподдержку.

**Александр Макаров**

Принципиальных отличий не вижу. Есть разница в специфике программ по обеспечению безопасности и надежности передачи данных. Казалось бы, решения у всех схожие, однако всегда присутствует своя

специфика. Чтобы получить надежную систему на известных решениях, нужен определенный опыт.

**Александр Крахмалев**

Есть определенная специфика для ПО систем безопасности. Это прежде всего надежность и защищенность от несанкционированных действий. Функциональная направленность — ничего лишнего и постороннего, что могло бы отвлекать пользователя (оператора) от выполнения главной задачи.

**Антон Садов**

Надежность в работе и критичность ошибок и сбоев — это первое. При подборе системы безопасности конечный клиент рассчитывает на стабильность системы и некую защищенность. Если заявленные параметры не работают, зачем это использовать? Среди особенностей программной системы видеонаблюдения можно отметить потреб-

ность клиентов видеть в одном продукте все возможности, реализованные в нескольких других системах, или идеи, реализованные отдельными производителями камер. Что касается программного обеспечения «Линия», нашим руководством дополнительно преследуется цель доступности программы для клиентов как в финансовом плане, так и в удобстве настройки, эксплуатации и освоения программы пользователями. Как говорится, будь проще — и люди к тебе потянутся.

**Вячеслав Тесаков**

Для программных разработок в отрасли систем безопасности требуется высокий уровень компетенций. Специалистов, которые обладают таким уровнем компетенций, очень немного. Чтобы написать программу, которая бы помогала обеспечивать безопасность на объекте, нужно владеть знаниями во многих смежных сферах. Кроме того, нужен хороший постановщик задач.

