БЕЗОПАСНИКИ И IT-ШНИКИ. ОНИ ТАКИЕ РАЗНЫЕ, НО ВСЕ-ТАКИ ОНИ ВМЕСТЕ!

Юнисов Александр Александрович
генеральный директор
ООО «Видеомакс»

CCTV

Долгое время рынки систем безопасности (СБ) и информационных технологий (IT) развивались параллельно. В каждой из сфер были свои подходы и технологии, свои достижения и свои игроки. С годами информационные технологии заполонили все сферы нашей жизни. Это происходит как на бытовом уровне, так и на уровне отраслевых решений. Благодаря открытым стандартам, развитым технологиям и универсальным подходам в обработке данных IT становится базисом для решения любой задачи. Аналогичное происходит и с системами безопасности – IT-инфраструктура все больше заменяет специализированные решения. Самый яркий пример – системы видеонаблюдения *(рис. 1)*.

Взрывной рост сегмента IP-видеонаблюдения, который мы наблюдали последние несколько лет, был обусловлен тем, что все необходимое уже давно существовало: среда передачи данных – ЛВС, средство обработки данных – серверы. Аналогичные процессы, с некоторым запозданием, идут и в системах контроля доступа, и даже в охранной и пожарной сигнализации. Контроллеры СКУД уже давно подключаются по IP, а системы IP-оповещения начали активно теснить классические с прямым подключением динамиков.

Хорошо это или плохо? Ставить так вопрос – это значит идти против прогресса. С точки зрения развития СБ, конечно же, хорошо. «Безопасники» получили в пользование развитые технологии и решения, которые значительно упрощают и унифицируют построение инженерных систем на объектах. Появляется возможность простой интеграции с другими системами, интеграции в систему «интеллектуальное здание», совместного использования единой IT-инфраструктуры. Но если внимательно присмотреться к рынку СБ и IT, подходам к проектированию, правилам работы, способу решения задач, то мы увидим множество различий. Эти различия могут быть существенными, а противоречия сложно разрешимы. В нашей статье мы постараемся выявить такие противоречия, предоставить пищу для размышлений и частично наметить варианты адаптации подходов и различных решений.

Статья от лица участника рынка СБ, поэтому сразу просим прощения за перекосы в сторону «безопасников».

Рис.1. IP-видеонаблюдение – пример перехода на IT-технологии в системах безопасности

ПОДХОДЫ К РАБОТЕ. ХУДОЖНИКИ ИЛИ РЕМЕСЛЕННИКИ?

Прежде чем переходить к тонким технологическим и техническим моментам, давайте разберемся, кто такие «безопасники» и «IT-шники» и почему мы такие разные.

В России с давних времен сфера СБ была тесно связана со спецслужбами, с государством, и, соответственно, тяготела к закрытости, к секретности, к недоверию. И в наше время этот след еще чувствуется. В дополнение, чтобы создать хорошую систему защиты от врагов, нужно думать как враг, нужно видеть в каждом врага, и только тогда будет возможно построить надежную систему безопасности. Первое, о чем думает специалист по безопасности, берясь за проект, – какие угрозы стоят перед объектом заказчика, и какая тактика охраны будет эффективна в борьбе с этими угрозами.

Сфера IT всегда развивалась в открытом общении специалистов. Она подчинена жестким стандартам и правилам построения. Есть типовые общепринятые решения, которые все участники открыто и повсеместно внедряют.

Рассмотрим основные отличия *(таблица 1)*.

Из сопоставления видно, что различий много. Мы живем на разных планетах. Мы разные на ментальном уровне. Может, тогда и не стоит дружить? Может, «безопасникам» отстраниться и разрабатывать свои стандарты и технологии? По разным причинам этого точно не случится. Одна из них связана с тем, что рынок IT на порядок обширнее, чем рынок СБ. И нам в любом случае придется применять, а порой и адаптировать, технологии и решения IT-рынка для систем безопасности. Именно об этом мы и поговорим далее.

Табл. 1. Разница в подходе к решению задачи

БЕЗОПАСНИК	IT-ИНТЕГРАТОР
■ Творческий подход, нестандартные решения. Типовые инсталляции уязвимы ■ Отправная точка – анализ угроз и разработка тактики охраны ■ Доверительные отношения между заказчиком и подрядчиком. Конфиденциальный характер любого взаимодействия и документооборота ■ Высокая маржинальность, эксклюзивные и дорогие услуги ■ Поставил и забыл ■ Большое количество «нишевых» и вертикальных решений для различных объектов и специализированных задач	■ Шаблонные решения в соответствии со стандартами и датшитами ■ В приоритете техника, а как ее использовать – второстепенно ■ Принято зарабатывать на объемах и услугах сервиса ■ Поставить так, чтобы тебя не забыли

Табл. 2. Особенности ЛВС для разных задач

ЛВС ДЛЯ СБ И ВИДЕОНАБЛЮДЕНИЯ	КОРПОРАТИВНАЯ ЛВС ПРЕДПРИЯТИЯ
■ Постоянный трафик с данными одного типа ■ Для выделенной сети защита и шифрование не требуются – доступ физически ограничен доверенными лицами ■ Протяженные участки внешних сетей горизонтальных сегментов ЛВС. Например, видео на периметре ■ Децентрализация и распределенность. Точек подключения мало, но по всему объекту ■ Высокие требования по отказоустойчивости всех компонентов и участков сети – нет второстепенных участков сети	■ Структура трафика и объем данных сложно прогнозируем ■ Многократный запас полосы пропускания ■ Одна сеть для всего трафика ■ Назначение приоритетов типам трафика, управление, защита, контроль для критичных приложений и задач осуществляется на уровне умных коммутаторов ■ Высокая степень централизации. Все стекается в единый дата центр ■ Высокие требования по отказоустойчивости только для датацентра и магистральных каналов ■ Частое переоснащение, дооснащение, модернизация

Табл. 3. Сравнение серверов для разных задач

ВИДЕОНАБЛЮДЕНИЕ	КОРПОРАТИВНЫЙ СЕРВЕР
■ Один тип данных, одно приложение ■ Приоритет записи в работе с дисковой подсистемой ■ Работа в режиме реального времени. Важно принять и обработать данные без задержек – контроль целостности не имеет высокого приоритета ■ Ограниченное количество подключений	■ Разнообразные данные и задачи. Часто на одном сервере работают несколько приложений ■ Нет выраженного приоритета записи/чтения ■ Потеря или искажение части данных критичны ■ Большое количество подключений

СЕТЕВАЯ ИНФРАСТРУКТУРА. ОДИН ДЛЯ ВСЕХ, ИЛИ ВСЕ ДЛЯ ОДНОГО?

Никто не будет спорить, что использовать ЛВС для передачи информации в СБ удобнее, нежели прокладывать свои специализированные каналы связи. Хорошо, что мы уже отошли от этого! Насколько далеко? Давайте порассуждаем.

ЛВС для IT-инфраструктуры – это транспорт, кровеносная и нервная системы в одном лице, это основа, на которой базируется любая информационная структура. Создавая ЛВС, IT-интегратор планирует использовать ее для различного рода приложений и задач, что создает ему дополнительные трудности с расчетом и прогнозированием трафика, выбором оборудования и решений. Для систем безопасности ЛВС – это средство доставки известного и постоянного трафика из точки А в точку Б. В таком случае построение ЛВС – простейшая линейная задача со всеми известными. Попробуем сопоставить различия подходов *(таблица 2)*.

Казалось бы, ну сети-то мы используем одни и те же. Однако и здесь видна разница в требованиях, и подходы к проектированию ЛВС для видеонаблюдения должны быть иными. Если есть возможность, то ЛВС для СБ и ЛВС для остальной информационной сети стоит разделить. В сети для корпоративного использования следует заложить запас производительности, расширяемости, коммутаторы с возможностью назначения приоритетов типу трафика, управления, диагностики, шифрования и т. п. А для того же видеонаблюдения, как это ни странно, часто достаточно надежных простых коммутаторов и качественных компонентов периферийной СКС. В случае необходимости, соединение сетей возможно на коммутаторах уровня ядра сети.

СЕРВЕРЫ. СПЕЦИАЛИЗИРОВАННЫЕ РЕШЕНИЯ ДЛЯ СБ

Серверы, и в целом станционное оборудование системы безопасности, имеют ту же самую техническую базу, что используется для корпоративных приложений. Каких-то специализированных решений именно для систем безопасности, где на уровне схемотехники учтена соответствующая специфика, не существует. Опять же по причине того, что этот рынок слишком мал для создания отраслевых решений. Однако специфика применения серверного оборудования в системах безопасности все же есть. Перечислим кратко основные моменты на примере сервера для системы видеонаблюдения и сервера для работы с корпоративными базами данных *(таблица 3)*.

Задачи для серверного оборудования в СБ и IT довольно сильно отличаются. Значит ли это, что сервер, разрабатываемый для корпоративных приложений, не справится с задачами видеонаблю-

дения? Конечно, справится. Но будет ли подобное решение оптимальным? Скорее всего, нет. Заказчик переплатит за лишнюю производительность и функции, которые не будут востребованы для задач видеонаблюдения.

Сегодня на рынке СБ уже есть предложения от компаний, которые специализируются на создании серверных решений для видеонаблюдения. В основе те же самые компоненты, что и для серверов корпоративного класса, однако конфигурация их оптимизирована, а программное обеспечение настроено так, чтобы наиболее эффективно обрабатывать видеоконтент в системах видеонаблюдения.

ХРАНЕНИЕ ДАННЫХ. DAS ИЛИ NAS?

Вы спросите: ну какая же может быть специфика систем безопасности в хранении данных? Те же самые нолики и единички! С одной стороны, биты те же, а вот задачи по их хранению и доступу разные. В примере будет снова видеонаблюдение, как основной генератор данных в СБ.

Когда мы говорим о больших объемах информации, то в мозгу у IT-специалиста мгновенно рождается картинка в виде вместительного NAS (Network Attach Storage), который он при случае может использовать еще для чего-нибудь. Класс! IT-индустрия нам подарила такое удобное и универсальное решение для хранения всего и вся, почему бы его не использовать. Что же рождается в голове у «безопасника»? Правильно – «запихнуть» побольше дисков в сервер и хранить там видеоархив *(рис. 2)*.

Этот вариант называется DAS (Direct Attach Storage). Архаизм? Незнание новых технологий? Давайте разбираться.

Для чего создавался NAS? Основное назначение – многопользовательский доступ и возможность хранения больших массивов разнообразных данных в одном месте.

В большинстве случаев NAS используют для хранения всевозможных бэкапов – резервных копий баз данных, файлов с пользовательских ПК, копий резервного восстановления операционной системы и т. п. Если связь с NAS кратковременно потеряется – ничего страшного, запишем очередной бэкап немного позже.

Это все совсем не похоже на то, что нужно для видеонаблюдения. В видеонаблюдении одно приложение пишет один тип данных, у которых равный приоритет. Потеря доступа к хранилищу недопустима – в первую очередь для записи, но и постоянный доступ к архиву для некоторых задач обеспечения безопасности может быть очень важен. Все перечисленные выше преимущества NAS в системах видеонаблюдения просто-напросто не востребованы. А отдаление дискового массива от сервера по локальной сети не позволяет гарантировать непрерывную и надежную запись.

РЕЗЕРВИРОВАНИЕ. ЗАДАЧА ОДНА, РЕАЛИЗАЦИЯ РАЗНАЯ

Надежность и отказоустойчивость станционного оборудования для систем видеонаблюдения требуется априори. Аналогичное требование существует и для корпоративных серверов предприятия. Вот мы и нашли точку соприкосновения! Каким же образом в IT-сфере принято защищать сервер от выхода из строя?

Если сервер выходит из строя, то работу берет на себя резервный сервер. Все это настраивается на уровне специальных приложений виртуализации, когда в основе виртуального сервера могут быть два-три и даже больше реальных серверов. Такие сложности оправданы тем, что IT-специалисту нужно защитить операционную систему от выхода из строя железа и обеспечить непрерывность работы виртуальной среды, в которой может быть запущен не один десяток приложений с различным уровнем критичности отказа. К тому же, перезапуск приложения нередко оказывается сложной процедурой с верификацией баз, проверкой целостности данных, переподключением клиентов и т. п.

Любой «безопасник» знает, что в серьезных VMS есть функция резервирования серверов. Зачем же она нужна, если в IT уже все есть: сделал виртуальный сервер из двух реальных, и готово? Однако, редко кто в СБ использует виртуализацию. Это не связано с тем, что в СБ нет хороших IT-специалистов (хотя по-честному – есть и такая проблема). Основная причина – в виртуализации просто нет необходимости. На видеосерверах работает одно приложение, и при выходе из строя сервера нужно обеспечить переход камер к другому в рамках единственного приложения. Кратковременная потеря камер при переключении в большинстве случаев не критична. Именно поэтому проще поставить пару галочек в специализированном ПО видеонаблюдения и настроить резервирование средствами VMS, не прибегая к сложной настройке виртуальных сред.

МОНИТОРИНГ И ОБСЛУЖИВАНИЕ

Подходы к мониторингу состояния компонентов системы безопасности и обслуживанию в СБ и IT также различны *(рис. 3)*. Хотя, казалось бы, компоненты те же самые, и почему не исповедовать единые стандарты. Ограничимся простой констатацией фактов без объяснения причин. Либо можно сказать: «Так сложилось исторически!». Кратко перечислим основные факты *(таблица 4)*.

Рис. 2. Классическое решение для СБ – локальные дисковые массивы для хранения архивов в видеосерверах

Рис. 3. Обслуживание СБ принято осуществлять в рамках договора по утвержденному регламенту

Табл. 4. Условия для обслуживания

СИСТЕМА БЕЗОПАСНОСТИ	IT-ИНФРАСТРУКТУРА
■ Круглосуточный мониторинг ■ Низкоквалифицированные операторы ■ Обслуживание периодическое по регламентам ■ Устранение неисправности в рабочее время дежурным техником либо обслуживающей организацией в рамках срока, оговоренного договором ■ Закрытые системы без возможности выдачи уведомлений куда-либо и удаленной перенастройки	■ Круглосуточный мониторинг и оперативное устранение любых сбоев высококвалифицированным персоналом ■ Мгновенное уведомление о любых сбоях ответственных специалистов и руководящего состава ■ Удаленное устранение сбоев, перенастройка, администрирование

Это портрет классической системы безопасности и того, как работает IT-инфраструктура. Можно подумать, что в СБ просто бардак. Однако, причина тому – особая специфика закрытой системы и разные задачи. Вышеприведенные факты стоит учитывать при выборе решений по мониторингу и планировании регламентов обслуживания будущей системы. Часто бывает так, что проектировщик системы безопасности закладывает решения по мониторингу и уведомлению об аппаратных сбоях, характерные для IT-инфраструктуры. Но, в итоге, это не работает, а причина тому – простое отсутствие связи с внешним сервером мониторинга. Можно было бы вверить мониторинг оператору – он же у нас круглосуточно присутствует на посту охраны. Но оператору видеонаблюдения нужно смотреть в камеры и выявлять злоумышленников. Ему просто некогда смотреть в монитор состояния аппаратной части системы и отслеживать загрузку процессоров, дисков и т. п. Да и вряд ли он там что-то полезное для себя найдет – это не его работа. В конечном итоге не редки случаи, когда без должного внимания станционное оборудование СБ начинает давать сбои.

Учитывая особенности организации мониторинга в СБ, следует выбирать иные решения по организации уведомления о сбоях, разрабатывать системы, которые прогнозируют неисправность, уведомляют оператора в удобном и привычном для него виде, где написано, что ему нужно сделать и кому передать информацию. И такие решения есть на рынке. Отдельные производители VMS даже встраивают в свои программные продукты средства мониторинга. У некоторых производителей специализированных серверных решений для систем видеонаблюдения вы найдете такие приложения. Это еще один довод в пользу специализированных серверов для систем безопасности.

ГЛАВЕНСТВО МЫСЛИ НАД ТЕХНОЛОГИЕЙ

Мы с вами рассмотрели несколько аспектов построения систем безопасности, когда прямое использование типовых решений из IT-сферы не оптимально, не удобно и порой даже негативно сказывается на характеристиках будущей системы безопасности. Возможно некоторые аспекты выглядят спорно, возможно, наоборот – вы добавили бы еще пару примеров. Будем считать успехом этой статьи, если в будущем, при построении систем безопасности, вы начнете задумываться: а так ли хорошо то или иное решение, которое нам предлагают поставщики из сферы IT-технологий, и на сколько это соотносится с тем, как работает система безопасности, как она эксплуатируется, какие задачи решает.

Что касается оборудования, получается, что кроме серверов для систем видеонаблюдения никто нам ничего специализированного не предлагает. Неужели рынок СБ настолько мал, что не удостоен внимания крупных игроков на рынке IT? Некоторые подвижки уже есть, особенно в части хранения видеоданных. Производители HDD предлагают нам специализированные диски. Все больше появляется NAS, оптимизированных для работы в видеосистемах. Рынком систем видеонаблюдения заинтересовались производители RAID-контроллеров. Возможно нам стоит ждать специальных прошивок для работы с видеоархивом.

Несмотря на эти отдельные факты, кардинальных изменений и разработки специальных протоколов и стандартов мы вряд ли увидим. Остается только лишь адаптировать имеющиеся технологии к требованиям и особенностям систем безопасности и учитывать эту специфику в процессе проектирования.

Последнее, что стоит отметить. Несмотря на всю указанную специфику сферы СБ, IT-компании смело идут в проекты построения систем безопасности. Более того, в больших проектах мы уже не встретим «безопасников» в чистом виде. Нередко мы видим и проблемы, с этим связанные, когда забывают о том, зачем собственно ставится система, и вместо проработки тактики охраны занимаются осваиванием бюджета и установкой большого количества оборудования, которое оператору не то что не помогает, а часто и мешает. Поэтому для IT-компаний крайне важно осознать особенности и специфику задачи обеспечения безопасности объекта. Этого им и пожелаем!