«К утру чтобы все работало»

Отправляясь на первую встречу с заказчиком, поставщик систем безопасности никогда не знает заранее, с кем придется иметь дело — со службой безопасности или ИТ-департаментом. При том что стратегия принятия решений у этих специалистов может отличаться радикально. Читатели журнала RUБЕЖ поделились личным опытом взаимодействия с обеими службами, что может пригодиться при подготовке коммерческих предложений.

Подготовили: Евгения Лысенко, Александра Найденова, Наталья Афонина

Антон Увакин
главный технический эксперт, ООО «ЛУИС+»

Я несколько лет веду обучающий курс по IP-видео в нашем учебном центре в рамках Академии LTV и могу сказать, что у сотрудников служб безопасности есть определенные пробелы знаний в области IP-технологий. В отличие от них, специалистам ИТ-служб проще начать разбираться в работе систем IP-видеонаблюдения, так как они знакомы с понятием IP-адресации и процессом подключения камер к серверам. Дополнительных вопросов и сложностей у них возникает меньше, потому что начальный набор знаний позволяет им быстро осваивать эту новую сферу деятельности.

В качестве примера типовой ошибки сотрудников служб безопасности можно привести ситуацию, связанную с настройкой системы IP-видеонаблюдения: подключают IP-камеру к NVR, а система не функционирует. Приходится объяснять, что нужно назначить IP-адреса для каждого из устройств, прописать эти адреса, чтобы устройства видели друг друга, ввести логины и пароли и т.д.

Еще один пример того, как ИТ-отдел может помешать работе безопасников. Есть множество ситуаций, в которых интересы и задачи СБ и ИТ-департаментов пересекаются. Случается, что система видеонаблюдения использует порты, которые ИТ-отдел по соображениям безопасности закрывает. В некоторых компаниях есть обязательное условие использования антивирусных программ и фаерволов, тогда как для системы IP-видеонаблюдения это является преградой — видеопоток может блокироваться. Потоки видеокамер всегда довольно емкие, нужен широкий канал, а специалисты ИТ порой ограничивают канал для всей системы видеонаблюдения до двух мегабит в секунду. В таком случае специалистам служб безопасности приходится предпринимать усилия, чтобы понять суть проблемы и в дальнейшем решить вопрос с ИТ-специалистами. Часто приходится перенастраивать оборудование, организовывать более широкий канал либо строить отдельную сеть для видеонаблюдения.

Александр Большедворов

генеральный директор, ТД «Амиком Урал»

На этапе создания проекта мы взаимодействуем с тремя сотрудниками — генеральным директором, сотрудником службы безопасности и ИТ-специалистом. Каждого из них интересует свой комплекс вопросов. Директора интересует цена, руководителя службы безопасности — характеристики и качество системы, ИТ-специалист выступает в качестве связующего звена новой системы с существующими процессами в организации.

Мы в своей работе не раз сталкивались с заблуждениями ИТ-специалистов. Например, при создании периметральной системы видеонаблюдения на объектах с большой протяженностью участков мы часто предлагаем использовать промышленный Wi-Fi. Очень многие ИТ-специалисты в ответ заявляют, что создать качественную Wi-Fi-сеть невозможно, на расстояние более 100 м сигнал передаваться не будет. Но мы на своем опыте знаем, что это более чем реально, особенно для заводов. Мы предлагаем не прокладывать провода по цехам, а использовать Wi-Fi, тем самым экономя деньги на проводах и стоимости прокладки.

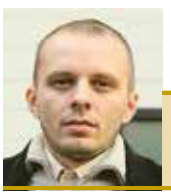
Например, недавний случай. При создании системы видеонаблюдения мы закладывали в проект экранированный кабель. В комментариях к проекту ИТ-специалист указал, что прокладка такого кабеля влечет за собой удорожание проекта, что нет необходимости в таком кабеле, нужно прокладывать обычную витую пару, которая на 20% дешевле. Наш аргумент для директора был прост. Расстояние было около 3 км, таким образом, цена вопроса составила 6 тысяч рублей. Если бы по причине желания сэкономить появились помехи на линии, то нам пришлось бы перекладывать 3 км кабеля, а это уже совсем другая цена вопроса.

Другое распространенное заблуждение, что систему видеозаписи необходимо делать на серверах. В некоторых задачах это действительно так, но опыт показывает, что под каждую задачу должно быть индивидуальное решение. При построении небольших систем вполне подходят видеорегистраторы. Или устанавливать на пост охраны компьютеры для отображения видеосигнала с камер — охранник будет использовать его не в служебных целях, что понижает надежность системы. Очень сложно бывает переубедить клиента не устанавливать компьютеры, а воспользоваться готовым решением на базе регистраторов.

У сотрудников службы безопасности тоже бывают свои заблуждения. Некоторые измеряют качество системы видеонаблюдения количеством пикселей. Приходиться объяснять, что каждая камера предназначена для конкретной задачи. В лифте или другом небольшом помещении нет смысла устанавливать 3- или 5-мегапиксельную камеру. Задачи, которые ставятся перед камерой, можно решить и с меньшим разрешением. Нужно понимать, что камера с высоким разрешением влечет за собой увеличенную нагрузку на сеть и уменьшает глубину архива. Мы стараемся донести до заказчиков, что каждая камера и задача уникальны и нет универсального решения. Самый действенный способ при этом — показать клиенту снимки с камеры в схожих условиях, при этом клиент на стадии проектирования представит, что он получит в итоге.

Можно сказать, что сотрудникам безопасности порой нелегко понять все аспекты современных систем, так как многие не имеют ИТ-образования. По этой причине они и привлекают ИТ-специалистов как экспертов для подбора системы. В 90% случаев на должность в службу безопасности приходят бывшие сотрудники внутренних органов. Их знания в ИТ-сфере ограничены, и только 10% сотрудников имею специальное образование.

Получается, что генеральный директор принимает окончательное решение, оценивает убытки и целесообразность затрат на систему, ИТ-специалист представляет собой доверенного консультанта, к чьему мнению прислушивается руководитель, а генератором и инициатором создания систем безопасности является СБ. Кроме того, сотрудник безопасности — это еще и связующее звено между директором и нами как исполнителем, на него же возложена обязанность составления технического задания. Специалист службы безопасности принимает готовую систему, потому что именно он является конечным потребителем этой системы.



Павел Грашин

руководитель отдела маркетинга, ООО «ВижнПро»

В 70–80% случаев мы взаимодействуем с ИТ-службами компаний-заказчиков, гораздо реже — со службами безопасности. Эти подразделения в рамках одной организации чаще всего сильно различаются. Обычно в СБ работают бывшие сотрудники правоохранительных органов, а в ИТ — инженеры или программисты. Разница заключается в психологии людей. Программисты действительно хотят разобраться в технической стороне проекта, повышают свою грамотность, а у безопасников такой подход: «Я ничего не знаю, но чтобы к утру все было сделано». Обычно это никак не влияет на работу, представители служб безопасности говорят, что их не интересуют подробности, им важно получить готовый результат. Однако бывают и неприятные случаи, когда представители СБ заявляют: «Я не учился и учиться не хочу», но пытаются сами поучать наших специалистов.

Уровень ИТ-грамотности клиентов рынка технических средств безопасности самый разный. Некоторые заказчики своими познаниями могут заставить «подвиснуть» даже производителей или разработчиков оборудования, а некоторые не знают элементарных вещей. Например, недавно мы столкнулись с проектом перевода некоего объекта с аналогового на IP-видеонаблюдение. Так вот, в документации были абсолютно детские ошибки вроде неправильно рассчитанного трафика через существующую сетевую инфраструктуру. Причем в некоторых узлах сети превышение по максимально допустимому трафику шло не на несколько процентов, а в разы! При этом проект подготовили сотрудники ИТ-отдела с инженерным образованием.

Встречаются и обратные примеры. У нас был случай, когда по инициативе одного из наших постоянных клиентов очень уважаемый производитель оборудования внес изменения в прошивку некоторых моделей камер, то есть инициатива снизу оказалась более чем актуальной.

Безусловно, поставщикам систем безопасности необходима ИТ-грамотность хотя бы на базовом уровне. Иначе в ситуациях, когда заказчики присылают тендерную документацию, в которой аналоговый регистратор 4-летней давности предполагается как-то ставить вместе с новейшими 5-мегапиксельными IP-камерами и подключаться через роутер D-Link за $50, мы просто не знаем, что делать.

Андрей Васильев
директор по развитию бизнеса, ТД «Видеоглаз»

Реализуя наши проекты, продавцы технических средств безопасности в равной мере взаимодействуют со службами безопасности и ИТ. Начальники СБ, как правило, не разбираются в ИТ, не понимают технических вещей на должном уровне, а ИТ-специалисты более компетентны и глубоко проникают в поставленную задачу. Сегодня, чтобы работать на рынке систем безопасности с крупными проектами, ИТ-грамотность необходима, без взаимодействия с ИТ-специалистами просто не обойтись. При общении с ИТ нам необходимо быть более грамотными и подкованными, иначе айтишники просто не будут с нами работать.

В службе безопасности чаще всего работают люди, которые сидят на своем месте в одной и той же должности уже много лет или переходят на такую же должность из компании в компанию. И благодаря этому у них нарабатывается определенный опыт или появляются подрядчики, которые сотрудничают с СБ на взаимовыгодных условиях и решают все необходимые задачи.

Айтишники, как правило, имеют специальное образование. А вот при взаимодействии с начальниками службы безопасности иногда начинают возникать проблемы по причине их некомпетентности и недостаточного уровня знаний. Например, люди из СБ хотят установить системы безопасности какой-то конкретной торговой марки и не готовы рассматривать другие варианты. Из-за этого возникает много неприятностей, так как невозможно объяснить, что другие системы могут быть выгодней по цене и техническим характеристикам. Если человек из СБ всю жизнь ставил системы только одного бренда, знакомиться с другими он не готов. Типичный безопасник имеет богатый жизненный опыт, на котором и строит работу. В похожей ситуации ИТ-специалист, как правило, начинает рассуждать логически, он готов к тому, что нужно доказать, обосновать свое предложение как надежное и выгодное. Он привык работать в условиях, когда у заказчика (директора компании) есть выбор.

ИТ-неграмотность встречается на рынке техсредств безопасности нередко. И в круг наших задач при работе с заказчиками входит помощь в устранении, а часто — и в предотвращении распространенных ошибок.

Михаил Бялый
генеральный директор, ТД «Актив-СБ»

Мы работаем с инсталляторами, крупными предприятиями, конечными пользователями, физическими лицами и предприятиями. В меньшей степени мы осуществляем продажи через интернет-магазины. Уровень ИТ-грамотности на рынке технических средств безопасности оценивается нами по-разному: если изначально проект ведет ИТ-специалист, то с уровнем грамотности все нормально. Если проект ведут те, кто занимается системами безопасности, мы сталкиваемся с тем, что уровня знаний им хватает только для небольших объектов. Хотя в целом этап новизны для систем безопасности пройден. Никого не удивляют ни IP-камеры, ни их настройка. Многие сервисы, такие как P2P, позволяют упростить настройки при переадресации портов, внешних адресов.

Парадокс, но иногда высокий уровень ИТ-грамотности мешает человеку в работе. Мы продавали систему Trassir, собранную на Linux. Благодаря использованию Linux изделие удалось значительно удешевить, так как он бесплатный и требования к ресурсам у него минимальные. Если бы тот же самый сервер был собран на Windows, то нам бы потребовалось оплачивать лицензию Windows и использовать более дорогие комплектующие. Но покупатель сервера расстроился из-за пустой начинки и решил, что его обманули. Мы объяснили покупателю: он приобретает готовое изделие, которое позволяет гарантированно записывать и воспроизводить видео с девяти камер. Это решение было оптимизировано под поставленные задачи. Будь оно построено на другой системе, расходы и бюджет потребовались бы совершенно другие. Однако подобное положение дел покупателя не устроило. Его знания помешали ему взглянуть на решение с другой стороны. Обычные наши покупатели не лезут внутрь готовых изделий. Главное, чтобы цена устраивала их и заказчика.

Если говорить о том, кто должен вести проект по системам безопасности, то это будет СБ. Потому что в первую очередь тут решаются вопросы безопасности: какую камеру и где устанавливать, какой функционал она должна иметь, какая реакция должна быть. А если мы говорим об информационной безопасности, то компетентнее будет ИТ-директор с его пониманием модели угроз и способностью самостоятельно принять меры противодействия.

Когда на одного специалиста пытаются повесить обязанности другого, происходит неразбериха. ИТ-директор с наименьшей вероятностью будет компетентен в вопросах технической безопасности. Он не будет иметь дело ни с чем, что не относится к формату IP. Правда, сейчас появились новые аналоговые форматы (HD-CVI, HD-TVI). Камеры, работающие в этих форматах, могут передавать изображение разрешением 1080p, хотя не являются IP-устройствами. Вот тут и возникает вопрос, смогут ли их полюбить айтишники?

ИТ-специалистов у нас в стране значительно больше, чем безопасников. Существуют факультеты и даже целые институты, обучающие ИТ-грамотности. А вот уровень знаний по системам технической безопасности на фоне ИТ-сегмента достаточно низок. Хотя это тоже отдельная сфера знаний. Система безопасности — это не просто установка камер, это определенная их настройка под каждую «сцену» на объекте. Необходимо разбираться в объективах, ИК-подсветке и прочих тонкостях. У тех же ИТ-специалистов часто таких знаний нет, заказ на установку системы видеонаблюдения они получают, включив ее в смету как дополнительную услугу за небольшие деньги.

В случаях, когда системы видеонаблюдения решают маркетинговые задачи, например в ритейле (наблюдение за очередью, подсчет людей), представители заказчика, особенно ИТ-специалисты, должны советоваться с менеджерами или технарями компаний — продавцов систем. Мы работаем с сетью магазинов, в которой за установку систем видеонаблюдения отвечают айтишники, и они привлекают к решению поставленных задач нашего технического директора. Тот лично выезжает на объект и совместно с ИТ-отделом определяет весь состав и функционал системы. Таким образом, ИТ-специалисты получают опыт в построении систем безопасности и используют его при установке систем в остальных магазинах.