ТЕМА НОМЕРА

СВЯЗАННЫЕ ОДНОЙ ЦЕЛЬЮ

Круглый стол по теме интегрированных систем безопасности. Участники нашего круглого стола: **Андрей Бедрань**, руководитель направления информационной безопасности департамента сетевой интеграции группы ЛАНИТ; **Аркадий Прокудин**, заместитель руководителя отдела информационной безопасности компании «АйТи»; **Алексей Морозов**, генеральный директор ООО «Конструкторское бюро систем связи», группа компаний АСБ; **Юрий Жуковский**, директор по развитию бизнеса компании «АРМО-ЛАЙН».

Тема интегрированных решений в последнее время не сходит со страниц журналов. Некоторые говорят о том, что это всего лишь дань моде, другие настаивают на необходимости перехода на интегрированные системы. Каждый в этом споре по своему прав, а потому истины в одной инстанции все равно не найти. Но вот внести ясность в вопросы целесообразности применения таких систем для решения конкретных задач и помочь правильно подойти к выбору компонентов возможно. С этой целью мы пригласили специалистов ведущих интеграторов рынка информационных технологий и технических средств обеспечения безопасности. Ведь данная тематика актуальна для всех независимо от сферы ее применения. К тому же безопасность организации не будет надежной без одного из этих компонентов.

1. Можете ли вы разделить объекты на две группы, одна из которых спокойно «проживет» на разрозненных системах безопасности, а для вторых интеграция систем реально необходима? Если да, то перечислите, пожалуйста, критерии такого разделения и поясните их.

А. Морозов. Скорее, объекты можно разделить на те, которые нуждаются в комплексной защите, и те, безопасность которых вполне обеспечивается отдельными подсистемами. В пользу такого вывода на бытовом уровне говорит простой здравый смысл, а на юридическом – положение об адекватности системы безопасности принятым моделям угроз проекта закона о противокриминальной защите (ФЗ РФ «О технических средствах обеспечения противокриминальной защиты объектов и имущества»). Среди объектов, нуждающихся в комплексной защите, выбор всегда будет в пользу интегрированных систем. Главный аргумент – более высокий уровень обеспечения безопасности при одинаковой стоимости.

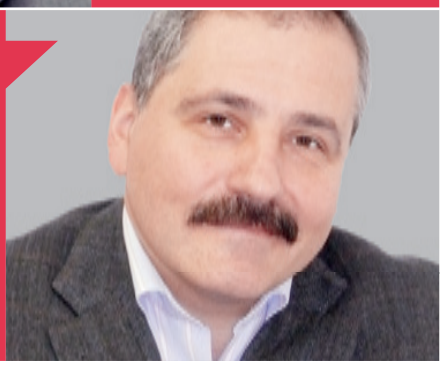
Ю. Жуковский. Действительно, в любом случае нужно руководствоваться здравым смыслом. И все же в качестве основных критериев такого разделения я бы отметил масштаб и сложность оснащаемого объекта. Для небольших офисов интеграция систем безопасности будет совершенно излишней. И наоборот, в крупном офисном здании или торговом центре, где работает и передвигается большое число людей в холлах,

Андрей Бедрань,
руководитель направления информационной безопасности департамента сетевой интеграции ЛАНИТ

Аркадий Прокудин,
заместитель руководителя отдела информационной безопасности компании АйТи

Алексей Морозов,
генеральный директор ООО «Конструкторское Бюро систем связи», Группа компаний «АСБ»

Юрий Жуковский,
директор по развитию бизнеса компании «АРМО.-ЛАЙН»



атриумах, коридорах, обеспечить безопасность персонала и посетителей силами разрозненных систем невозможно. Здесь интегрированная система безопасности – наиболее оправданное решение.

А. Бедрань. В случае с информационной безопасностью под интегрированными системами могут пониматься, во-первых, компоненты прикладных механизмов информационной безопасности, которые предусматривают интеграцию между собой, а во втором случае – механизмы безопасности, которые изначально присутствуют в «самописных» системах (например, наличие SSL в портальной теме). И так как сегодня мы будем говорить о механизмах интеграции средств обеспечения информационной безопасности и эффективных схемах реализации, то разделять объекты защиты на две, три и более группы нецелесообразно. Дело в том, что практически невозможно обеспечить требуемый уровень безопасности одним механизмом защиты. Несколько средств защиты с большой долей вероятности можно интегрировать и получить от этого выгоду.

2. Поскольку применение интегрированных систем безопасности не регламентируется государством, скажите, пожалуйста, на каких объектах их использование полностью оправданно и почему?

А. Бедрань. С нашей точки зрения, применение интегрированных систем безопасности оправданно на всех типах объектов. Это не только снижает стоимость владения системой безопасности, но и повышает эффективность работы отдельных механизмов безопасности.

Ю. Жуковский. По нашему опыту, в первую очередь к таким объектам относятся высотные здания, к которым предъявляются повышенные требования по безопасности в связи со сложностью эвакуации людей при пожаре и других чрезвычайных ситуациях. На таких объектах имеет смысл говорить об интеграции систем пожарной сигнализации и оповещения с системой видеонаблюдения, которая обеспечит визуальный контроль за происходящим. Например, система поможет понять, все ли сотрудники эвакуированы с опасных этажей здания.

Помимо этого стоит отметить здания с многочисленными подземными этажами, с необычными архитектурными решениями (арки, купольные своды), а также объекты с большим трафиком и частыми скоплениями людей – такие, как аэропорты и вокзалы. Подобные строения требуют повышенных мер безопасности – и прежде всего потому, что там скапливается большое количество людей, а значит, интеграция систем в данном случае обязательна.

Мы рекомендуем клиентам устанавливать интегрированные системы безопасности (ИСБ) и на объектах с большим внешним периметром, включая складские и логистические комплексы. Охрана таких территорий подразумевает как минимум срабатывание охранной сигнализации при несанкционированном пересечении периметра с одновременным выводом изображения с телекамеры, а также автоматическим включением освещения в тревожной зоне.
Важную роль ИСБ играют на удаленных объектах, например, на электроподстанции, где не предполагается присутствие человека. Для передачи актуальной информации с такого объекта объединяются в единый охранный комплекс охранная и пожарная сигнализация, видеонаблюдение, контроль доступа и системы автоматики, все данные с которых передаются по одному каналу на центральный пульт управления.

3. Какие задачи позволяет решать современная интегрированная система безопасности – из тех, которые не доступны СБ с классической архитектурой?

А. Морозов. С вашего позволения я бы заменил слово «классической» на «традиционной». Термин «классический» по сути является синонимом абсолютного совершенства, в сравнении с которым остальное воспринимается как «неклассическое», второсортное. Но это не так и в отношении интегрированных систем, и особенно в отношении традиционных, которые при всем желании никак нельзя квалифицировать как совершенные.
По существу же вопроса можно сказать, что в принципе любую задачу обеспечения безопасности можно решать как традиционным способом, так и с применением ИСБ. Вопрос только какой ценой. Ценой в широком смысле слова, а не только стоимости конкретного оборудования. Хотя, если подумать, то экономическая сторона вопроса может служить универсальным критерием. Давайте рассуждать. Вот вы, заказчик, поручили мне спроектировать систему безопасности. При традиционном подходе я начинаю «собирать с миру по нитке» – подбирать комплектующие различных производителей, сопрягать их по номиналам электропитания и потребляемой мощности, габаритным и конструктивным особенностям, интерфейсам и функциональным характеристикам. А это все – время и деньги.
Далее. В ИСБ приборы выполняют, как правило, некий набор функций, а в неинтегрированных – одну-единственную. Значит, вместо одного устройства нужно ставить несколько.
Затем начинается этап комплектации. Какие-то компоненты есть на складе, для каких-то срок поставки – два месяца, что-то уже сняли с производства, нужно подбирать другое, повторно согласовывать проект. Опять время, деньги. Наконец все укомплектовали, смонтировали.

> СРЕДИ ОБЪЕКТОВ, НУЖДАЮЩИХСЯ В КОМПЛЕКСНОЙ ЗАЩИТЕ, ВЫБОР ВСЕГДА БУДЕТ В ПОЛЬЗУ ИНТЕГРИРОВАННЫХ СИСТЕМ. ГЛАВНЫЙ АРГУМЕНТ – БОЛЕЕ ВЫСОКИЙ УРОВЕНЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОДИНАКОВОЙ СТОИМОСТИ
>
> Андрей Бедрань

Теперь надо обучать специалистов заказчика. А производители у подсистем разные. Изучать и эксплуатировать несколько различных подсистем сложнее, чем одну. Значит, требования к квалификации специалистов будут выше. Дурак не справится, а умный дорого стоит. Опять время, деньги. В процессе эксплуатации оборудование, какое бы надежное оно ни было, не застраховано от отказов. Значит, надо иметь на собственном складе или искать запчасти у поставщиков. Поставщик для ИСБ – один, а для традиционных систем их целый список. И это только самый поверхностный анализ, но даже он позволяет «почувствовать разницу».

А. Прокудин. Интегрированная система выявляет инцидент безопасности на стадии его совершения, а не после проявления последствий. Стоит также заметить, что системы безопасности с классической архитектурой намного уязвимее в отношении вероятности вывода их из строя.

Ю. Жуковский. Поддерживаю коллегу в том отношении, что при использовании интегрированных решений сокращается время реагирования на событие, а также повышается информативность получаемой информации. В области систем физической безопасности, например при срабатывании охранных или пожарных датчиков, можно сразу же получить картинку с места событий и оперативно принять соответствующие меры. Кроме того, интегрированные системы безопасности обладают своего рода интеллектом, который позволяет выявить потенциально опасные ситуации и привлечь к ним внимание оператора, повышая тем самым эффективность защиты и минимизируя риски человеческого фактора.

А. Бедрань. Со своей стороны хочу резюмировать уже сказанное: современная интегрированная система безопасности способна на многое. Например, интеграция системы обнаружения и предотвращения вторжений (IPS/IDP) с системой управления уязвимостей дает возможность

существенно снизить количество ложных срабатываний при определении и блокировании атак.
Глобально ИСБ позволяет сделать макрокорреляцию разных событий безопасности. Это означает, что система сможет обрабатывать и использовать информацию от принципиально иных механизмов безопасности на основе уникальных правил корреляции. Вершиной «пирамиды» в данном случае будет являться система мониторинга и управления инцидентами безопасности (SIEM). На рынке широко представлены подобные решения от производителей ArcSight, EMC, Symantec, Q1 Labs.

4. Какие новые полезные функции и возможности появились у ИСБ за последние два-три года?

А. Морозов. Системы безопасности, в частности ИСБ, относятся к классу телеинформационных систем, поэтому новые возможности появляются на стыке телекоммуникационных и информационных технологий. В области охранного телевидения большие перспективы мы связываем с развитием тепловизионной техники, тепловизоров. По сравнению с обычными видеокамерами тепловизоры способны различать цели на больших расстояниях, в ночное время и в условиях сильных атмосферных помех – дождя, снега, тумана. В области информационных технологий уверенно заявила о себе и активно развивается тема встроенного видеоанализа. В области аудиотехнологий хочу отметить интеграцию в системы безопасности функций адресной речевой связи и речевого оповещения. Не того, ставшего уже привычным речевого оповещения в виде проигрыша заранее записанных аудиофайлов, а настоящего, живого оповещения от оператора. В сочетании с системой охранного телевидения речевая связь позволяет многократно повысить информативность ИСБ и, как следствие, уровень безопасности объекта. В области телекоммуникационных технологий большие перспективы связаны с развитием пассивных оптически сетей (PON). Такие сети позволяют упростить создание территориально распределенных структурированных кабельных систем, обеспечивают гигантскую пропускную способность, возможность создания ИСБ масштаба территориально распределенных образований.

Ю. Жуковский. Да, развитие идет на стыке технологий. Со своей стороны могу отметить, что в связи с бурным развитием мобильного Интернета все больше производителей интегрированных систем безопасности предлагают различные решения по осуществлению удаленного доступа к ИСБ. Скажем, тревожное видео с установленной в офисе телекамеры ИСБ может отправить на адрес электронной почты или на телефон. С любого мобильного устройства можно зайти через Интернет в систему и посмотреть, что происходит на объекте, например включена ли сигнализация. Дополнительные возможности в работе ИСБ связаны с появлением IP-камер с разрешением HD и Full HD, которые дают повышенную детализацию изображения. Функция сопровождения подвижных объектов позволяет с легкостью проследить за человеком по всему маршруту его передвижения, другая функция обратит внимание оператора на движение человека или машины в запрещенном направлении.

> «ИСБ ОБЛАДАЮТ СВОЕГО РОДА ИНТЕЛЛЕКТОМ, КОТОРЫЙ ПОЗВОЛЯЕТ ВЫЯВИТЬ ПОТЕНЦИАЛЬНО ОПАСНЫЕ СИТУАЦИИ И ПРИВЛЕЧЬ К НИМ ВНИМАНИЕ ОПЕРАТОРА, ПОВЫШАЯ ТЕМ САМЫМ ЭФФЕКТИВНОСТЬ ЗАЩИТЫ»
>
> Алексей Морозов

> «ИНТЕГРИРОВАННАЯ СИСТЕМА ВЫЯВЛЯЕТ ИНЦИДЕНТ БЕЗОПАСНОСТИ НА СТАДИИ ЕГО СОВЕРШЕНИЯ, А НЕ ПОСЛЕ ПРОЯВЛЕНИЯ ПОСЛЕДСТВИЙ»
>
> Аркадий Прокудин

5. А что в этом аспекте можно отметить в области информационной безопасности?

А. Прокудин. Сегодня ИСБ становятся интеллектуальными и, можно так сказать, самостоятельными. Последнее веяние западных и российских технологий – системы централизованного мониторинга и управления информационной безопасностью организации. Подобные решения позволяют управлять несколькими системами информационной безопасности из единого центра.

А. Бедрань. Конечно, системы приобретают все больше возможностей и становятся «умнее». Но все же «вкусного» функционала в нашей области появилось не так много, как хотелось бы. Почти все централизованные системы управления теперь могут делать простую мик-

рокорреляцию собранных логов со своих устройств. Они могут передавать тикеты в SIEM более высокого уровня. У многих мощных решений появились удобные API и внятные инструкции к ним. Это дало возможность более адекватно ставить задачу разработчикам прикладного софта при реализации комплексной системы информационной безопасности. Еще одной интересной особенностью является то, что многие производители решений безопасности уже «в коробке» имеют шаблоны интеграции с другими производителями. Конечно, это становится возможным только если технология работы стандартизирована (например, IPSec VPN на 3DES/AES), но идея все чаще находит применение. Она позволяет заказчику отойти от моновендорного подхода и выбирать решения, которые действительно эффективны.

6. На что советуете обращать внимание при выборе компонентов для построения интегрированных систем?

А. Морозов. Потребителю нужно прежде всего ознакомиться с характеристиками интегрированной системы в целом, понять, насколько она функционально соответствует его пониманию задачи обеспечения безопасности с учетом критерия адекватности и степени интеграции. Кому-то будет вполне достаточно функций охранно-пожарной сигнализации, кому-то требуется больше. Хорошей методологической основой для принятия решения может служить уже упомянутый ранее проект закона «О технических средствах обеспечения противокриминальной защиты объектов и имущества», где приведен полный перечень возможных функциональных характеристик ИСБ.

А. Бедрань. Безусловно, и тут я полностью поддерживаю коллегу, нужно обратить внимание на то, что дает система при реализации: интеграция без видимого практического результата бессмысленна. Далее следует проанализировать варианты интеграции с уже используемыми системами. Это даст возможность детально продумать схему интеграции и максимально задействовать существующую инфраструктуру.

Ю. Жуковский. Во всех случаях интеграции ключевую роль играет программное обеспечение. Поэтому особое внимание при выборе компонентов следует уделять именно возможностям и надежности управляющего ПО, а также совместимости охранного оборудования. Для этого производители интегрированных систем всегда предоставляют список поддерживаемых ими устройств с указанием марок и моделей. Среди наиболее известных брендов ИСБ я бы выделил Lenel Systems, Bosch Security, Esser by Honeywell и Cisco.

А. Прокудин. Немаловажно, на мой взгляд, при выборе компонентов ИСБ обратить внимание на эффективность конечного варианта системы безопасности и стоимость его обслуживания.

7. Насколько глубоко должна быть интегрирована СБ со стороны информационных систем и физических средств защиты? Какие данные или команды можно передавать сегодня между различными системами?

> «ПРИ ВЫБОРЕ КОМПОНЕНТОВ НУЖНО ОБРАТИТЬ ВНИМАНИЕ НА ТО, ЧТО ДАЕТ СИСТЕМА ПРИ РЕАЛИЗАЦИИ: ИНТЕГРАЦИЯ БЕЗ ВИДИМОГО ПРАКТИЧЕСКОГО РЕЗУЛЬТАТА БЕССМЫСЛЕННА»
>
> Юрий Жуковский

А. Прокудин. Я считаю, что интеграция СБ должна проводиться на уровне построения основной системы. Только при такой схеме можно максимально снизить риски потери или порчи информации в системах.

А. Бедрань. Если говорить об ИТ-безопасности, то глубина интеграции зависит от поставленной задачи. Как минимум нужно активизировать функции репортинга и мониторинга. В ряде случаев имеет смысл предусмотреть интеграцию систем физической безопасности с информационной системой.

Ю. Жуковский. С нашей точки зрения, глубина интеграции зависит в первую очередь от особенностей объекта. Например, для крупного складского комплекса «Авто-49» мы разработали и внедрили интегрированную систему безопасности, включающую систему видеонаблюдения, охраны периметра, контроля доступа, охранной сигнализации, ИТ-инфраструктуру. Для высотных зданий наиболее важна интеграция пожарной сигнализации и оповещения с системой охранного видеонаблюдения. Современные ИСБ позволяют задать практически любые сценарии реагирования на различные события в системе. Это может быть и автоматическая идентификация человека по карте доступа, и учет рабочего времени, и система распознавания автомобильных номеров, и интеграция с системами автоматики здания. При этом следует учитывать один особенно важный момент: все системы должны быть синхронизированы с высокой точностью. ■