Круглый стол

Технические аспекты построения системы информационной безопасности на промышленном предприятии

Мы продолжаем обсуждение темы защиты информационной инфраструктуры предприятия, в первой части которого участники поделились своим видением современных подходов к реализации технической политики информационной безопасности и затронули ключевые аспекты построения на программно-техническом уровне эффективной системы ИБ, а также обсудили основные вопросы, касающиеся политики управления ИТ-рисками.

В Круглом столе принимают участие:

Андрей Малакеев, генеральный директор, компания "Корпоративные Информационные Системы";
Кирилл Керценбаум, технический специалист, компания Symantec в России и СНГ;
Иван Мелехин, начальник отдела консалтинга, компания "Информзащита";
Владимир Баланин, руководитель отдела ИТ-безопасности, компания TopS BI;
Константин Кузовкин, начальник отдела технических решений департамента информационной безопасности, компания "Ай-Теко";
Дмитрий Шепелявый, руководитель технологического направления по продуктам безопасности, компания Oracle СНГ;
Вячеслав Статьев, директор по технологиям и решениям, компания "РНТ";
Олег Гудилин, руководитель отдела стратегического маркетинга, компания "Лаборатория Касперского";
Михаил Башлыков, руководитель группы инженеров информационной безопасности, компания КРОК;
Алексей Лукацкий, менеджер по развитию бизнеса, компания Cisco;
Наталья Базаренко, руководитель направления информационной безопасности, компания RRC EN.

– Какой должна быть доля расходов на безопасность в общих расходах на ИТ для компаний разного профиля деятельности? Зависит ли она от величины компаний? Как правильно рассчитать и обосновать необходимые вложения в защиту предприятия?

Андрей Малакеев, компания "Корпоративные Информационные Системы". Пока я о таком параметре не слышал. По крайней мере, мне неизвестны нормативы отчислений на ИТ-безопасность. Единственное, что можно утверждать по этому поводу, это то, что затраты на защитные мероприятия не должны быть выше, чем возможный ущерб. То есть, если возможный ущерб от реализации угрозы информационной безопасности предприятия составляет 100 руб., то нет смысла проводить мероприятия стоимостью 1000 руб. для предотвращения этой угрозы. Система оценки рисков как раз и позволяет получить информацию, необходимую для принятия решения о проведении тех или иных защитных мероприятий. От величины или профиля компании зависят типы угроз и размеры потерь, но сам подход от этого не меняется.

Кирилл Керценбаум, компания Symantec. Точный процент назвать довольно сложно, так как не существует определенных стандартов и правил на этот счет. Однако каждая компания способна, исходя из собственных задач, определить этот лимит и стараться придерживаться его при формировании долгосрочных ИТ-бюджетов. В общем случае, эта цифра может варьироваться от 0,2-0,3 до 3-5 % общего ИТ-бюджета. Часто эта доля больше зависит не от размера компании, а от рода деятельности, то есть от того, насколько риски ИБ угрожают бизнесу. Обосновать подобные расходы проще всего, проведя анализ рисков и произведя подсчет возможных потерь бизнеса в случае отсутствия системы ИБ.

Продолжение. Начало в REM № 2, 2008

Иван Мелехин, компания "Информзащита". Стастистика по данному вопросу существует, и она говорит о том, что затраты на безопасность в среднем составляют 5-10 % от ИТ-бюджета. Однако мне кажется, что измерять расходы на безопасность как долю от ИТ-бюджета не совсем корректно. Нужно четко понимать, о безопасности чего мы говорим. Если речь идет о безопасности ИТ-инфраструктуры или каких-либо базовых мерах защиты, то применение подобной статистики имеет смысл. Если же мы говорим о безопасности информации, или, в более узком смысле, информационных активов, то имеет смысл оценивать затраты на безопасность, исходя из стоимости самих активов. В качестве простейшей оценки бюджета на защиту активов "сверху" можно ориентироваться на размер страховой премии, в случае страхования соответствующих рисков. К сожалению, в силу неразвитости этой области страхования воспользоваться данным способом затруднительно. Единственной реальной возможностью оценить затраты остается анализ рисков, в той или иной форме. В зависимости от возможностей компании это может быть как сложная количественная методика, учитывающая большое число факторов, так и простейший качественный анализ, основанный на экспертном мнении участников. Необходимо только помнить о двух основных вещах: результаты анализа рисков должны быть привязаны к деньгам и утверждены руководством. Таким образом, можно предложить следующие варианты оценки бюджета на безопасность:

- на начальных уровнях информационной зрелости компании или в случае небольшой ценности информационных активов, можно использовать оценку затрат на базовые меры в размере 5 % от ИТ-бюджета;
- в случае высокой ценности информационных активов для компании оценку бюджета необходимо проводить, исходя из ценности этих активов.

Владимир Баланин, компания TopS BI. Для начала стоит заметить, что одной из характеристик уровня зрелости компании с точки зрения ИБ является факт финансирования этого вида корпоративных затрат в рамках отдельного бюджета. Бюджет на информационную безопасность можно разделить на две условные составляющие: бюджет на так называемый compliance (соответствие законодательству и требованиям регулирующих органов) и на средства защиты от угроз, характерных для данного типа предприятия (бизнеса). Если в области compliance оценить бюджет можно достаточно просто – есть требования и их нужно выполнять, соответственно, остается только выбрать подходящие средства защиты в зависимости от показателя стоимость/функциональность/управляемость, то вот в области защиты от характерных для предприятия угроз придется оперировать термином ROSI (Return on Security Investment). Упрощенно ROSI можно представить в следующем виде:

$$ROSI = \frac{(\text{Влияние риска, } \$ * \% \text{ снижения риска}) - \text{стоимость решения}}{\text{стоимость решения}}$$

Вполне очевидно, что при таком подходе будет выбрано решение, обеспечивающее наилучшее соотношение между снижением риска ИБ и стоимостью средств защиты. Разумеется, что в жизни формула будет не столь тривиальной, и для эффективного управления инвестициями в ИБ потребуется внедрение системы управления рисками.

Константин Кузовкин, компания "Ай-Теко". Пора уже прекратить битвы за бюджет между ИТ- и ИБ-подразделениями, так же как и спор о том, кому должна подчиняться служба информационной безопасности предприятия. На фоне общей тенденции встраивания продуктов ИБ в инфраструктурные и прикладные решения эти дебаты выглядят достаточно странно. Цель должна быть единой – создание эффективной и защищенной ИТ-инфраструктуры. Причем отдача будет достигнута только тогда, когда интеграционные процессы между ИТ- и ИБ-департаментами будут происходить не на уровне программных продуктов, а на уровне бизнес-процессов предприятия. Несколько отдельно стоят услуги по проведению аудита ИБ, сертификации и аттестации объектов информатизации. Эти услуги должны финансироваться отдельной статьей бюджета.

Дмитрий Шепелявый, компания Oracle. Экспертно определенная доля расходов на безопасность составляет приблизительно 10 % от бюджета на ИТ. От величины компании этот показатель не зависит. Применение того или иного средства защиты обосновано, если оно имеет неотрицательное ROI и, разумеется, в том случае, если этого требует законодательство.

Вячеслав Статьев, компания "РНТ". В этом вопросе необходимо учитывать обязательность выполнения тех или иных требований по безопасности и категории обрабатываемой информации. Если для государственных организаций номенклатура используемых технологий защиты определяется нормативной базой и перечнями сертифицированных решений ФСТЭК и ФСБ России, то для коммерческого сектора применение тех или иных технологий защиты с последующей аттестацией в большей степени обусловлено готовностью компаний их финансировать и их отношением к рискам и угрозам, которые при этом существуют. Хотя и для ком-

мерческих структур существуют обязательные требования, которые они должны выполнять применительно, например, к информации, содержащей сведения, отнесенные к категории государственной, служебной, врачебной тайны и персональным данным.

Основываясь на статистических данных и опыте практического внедрения технологий защиты, можно говорить, что в большинстве случаев прагматически обоснованная доля расходов на обеспечение информационной безопасности находится в диапазоне от 10 до 30 %, в зависимости от класса системы.

Олег Гудилин, компания "Лаборатория Касперского". Согласно последнему отчету американского Института компьютерной безопасности (CSI Computer Crime and Security Survey, 2007), более 20 % компаний тратят на информационную безопасность свыше 8 % от ИТ-бюджета, 26 % компаний ограничиваются 3-5 % и 35 % компаний тратят на ИБ не более 2 % своего бюджета, отведенного на ИТ. Это мировая практика. В нашей стране ситуация с затратами на ИБ сильно разнится с этими цифрами из-за высокого уровня пиратства и недостаточного понимания данной проблематики, но в крупных и успешных российских компаниях затраты на ИБ в целом совпадают с мировым уровнем.

– Насколько унифицированы в настоящее время средства защиты? Какие существуют стандарты и спецификации для систем безопасности российских предприятий и в чем их преимущества/недостатки по сравнению с зарубежными аналогами?

Михаил Башлыков, компания КРОК. Говорить об унификации средств защиты на сегодняшний день можно только в разрезе конкретных классов систем и способов их интеграции с внешними системами.

Для исторически зрелых классов (технологий) защиты, например, таких как системы обнаружения атак, определенная унификация существует. Так, некоторые IDS-системы способны подключать "чужие" сигнатуры атак. Кроме того, многие средства реализуют такие стандартные протоколы взаимодействия с внешними системами, как syslog и snmp.

Для других средств защиты, например инструментов построения шифрованных каналов связи, теоретически унификация существует, так как большинство данных решений реализует протокол IPSec, но практически заставить взаимодействовать между собой средства шифрования от различных производителей фактически невозможно.

В целом стоит отметить, что существует много международных организаций по стандартизации, которые активно разрабатывают унифицированные стандарты для средств защиты, и эти стандарты очень часто принимаются за основу вендорами; поэтому можно утверждать, что тенденция в сторону унификации средств защиты будет несомненно развиваться.

Если говорить о стандартизации в области ИБ в России, то в настоящий момент развитие стандартов идет в направлении наследования лучших мировых стандартов. Исключение составляют только стратегические области, например, стандарты на алгоритмы шифрования.

Вячеслав Статьев, компания "РНТ". В настоящее время для промышленных предприятий основная часть существующих ГОСТ'ов была разработана на основе соответствующих международных стандартов. Это, прежде всего, ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 27001, серия стандартов ГОСТ Р ИСО/МЭК 13335, серия стандартов ГОСТ Р ИСО/МЭК 15408 и ряд других.

Следует отметить, что существующие ГОСТ'ы имеют универсальный характер и не содержат в себе специфики проблемной области реального производства. Это обусловлено тем, что процесс адаптации международных стандартов в области PLM-технологий развивается не так быстро, как хотелось бы. При этом значительную долю рынка программных решений по реализации PLM-технологий для промышленных предприятий занимают разработки западных компаний, таких как SAP, Oracle, Dassault Systemes, Siemens PLM Software, PTC, Autodesk, MSC.Software, ABACUS, EMC и др.

Среди российских стандартов в области безопасности информационной поддержки жизненного цикла продукции следует отметить ГОСТ Р 52611-2005.

Что касается конкретных средств защиты, то наряду с традиционными – типа межсетевых экранов, антивирусов, криптошлюзов и криптомаршрутизаторов – наиболее широкое развитие получило встраивание российской криптографии в западные системы.

Константин Кузовкин, компания "Ай-Теко". Представляю справку. Средства защиты сертифицируются ФСТЭК (бывшая Гостехкомиссия), а средства криптографической защиты информации должны быть сертифицированы ФСБ. В следующих нормативных документах:

- Федеральном законе от 27 июля 2006 года № 152-ФЗ 27 "О персональных данных";
- Постановлении Правительства Российской Федерации от 15 августа 2006 года № 504 "О лицензировании деятельности по технической защите конфиденциальной информации";
- Специальных требованиях и рекомендациях по технической защите конфиденциальной информации (СТР-К ФСТЭК РФ)

требуется использовать для защиты конфиденциальной информации только сертифицированные средства защиты, в том числе и сертифицированные криптографические средства.

Основные действующие в РФ стандарты и руководящие документы по ИБ:

- Руководящие документы ФСТЭК (www.fstec.ru);
- ГОСТ Р ИСО/МЭК 15408, ГОСТ Р ИСО/МЭК 17799 и 27001 (российские аналоги (переводы) соответствующих международных стандартов);

Стандарт Банка России, в основу которого положены многие западные стандарты: CoBIT, ISO 27001 и др.

Сегодня уже поздно обсуждать, в чем преимущества и недостатки российских стандартов по сравнению с зарубежными. Речь должна идти о том, как организовать внедрение аналогов международных стандартов.

– С целью экономии средств можно ли строить систему защиты поэтапно, постепенно наращивая сложность, и в какой последовательности это следует делать?

Алексей Лукацкий, компания Cisco. Строить поэтапно не только можно, но и нужно – как говорится в известной русской поговорке, "нельзя съесть слона целиком". Этапность определяется результатами проведенного анализа рисков.

Иван Мелехин, компания "Информзащита". Абсолютно верно, систему защиты не просто можно, а нужно строить поэтапно. Ведь комплексная система информационной безопасности представляет собой сложный набор процедур, организационных мер и технических средств. Все составляющие этого комплекса находятся в сложном взаимодействии, и зачастую одни компоненты могут быть правильно реализованы только при условии успешного функционирования других. Например, неправильным бы было внедрять сложные процессы управления информационной безопасностью при отсутствии базовых средств защиты. Полномасштабный количественный анализ рисков очень сложно провести, не имея статистики по инцидентам за достаточно длительный период, а подобная статистика является результатом хорошо отлаженного процесса управления инцидентами, который, в свою очередь, не может нормально функционировать в случае отсутствия инвентаризации активов. И так далее... Таким образом, наиболее оптимально строить систему защиты поэтапно, начиная с базовых мер, средств и процессов и постепенно наращивая ее сложность и комплексность. Важным условием успешности поэтапного подхода является определение общей концепции развития системы на самых ранних стадиях и создание среднесрочной программы действий. Такой подход позволит плавно и управляемым образом повысить уровень зрелости системы информационной безопасности.

Кирилл Керценбаум, компания Symantec. Такая возможность существует, но вряд ли в данном случае можно говорить об экономии. Как и любое комплексное решение, система ИБ, будучи внедренной не до конца, может быть настолько малоэффективна, что вложенные в нее деньги не только не окупятся, но и могут дать прямо противоположный результат. Ведь основная задача комплексной системы ИБ – максимально снизить риски для бизнеса в процессе эксплуатации ИТ-инфраструктуры. Если же система внедрена не полностью, то уровень ее надежности может быть так мал, что она просто не позволит решить поставленную задачу на требуемом уровне.

Олег Гудилин, компания "Лаборатория Касперского". На практике поэтапное построение системы ИБ вполне допустимо и часто применяется. Нужно понимать, что внедрить весь комплекс систем защиты одновременно часто просто нереально именно из-за ограниченности ресурсов. Кроме этого, внедрение нескольких систем ИБ требует перестройки бизнес-процессов на предприятии, а это всегда занимает много времени. Но в случае выбора варианта поэтапного внедрения важно помнить, что любая недостроенная система не может быть эффективной, и затягивание ее построения на годы приведет к бесполезным затратам на поддержание неработающего в полную силу "долгостроя".

Наталья Базаренко, компания RRC. Безусловно, строить систему защиты поэтапно можно, особенно, если к этому располагает архитектура решений того или иного производителя. Последовательность наращивания функциональности задается порядком, в котором будут выстроены задачи по защите информации, в соответствии с их критичностью для бизнеса или функционирования предприятия. При этом важно учитывать возможность интеграции внедряемых решений, так как, в конечном итоге, на первый план выйдет задача снижения стоимости администрирования и владения этим решением.

Михаил Башлыков, компания КРОК. Только поэтапно и итерационно можно построить действительно эффективную систему защиты. Главное, чтобы в основе построения такой системы лежали обоснованные принципы и был разработан четкий план действий по их реализации. Обоснование должно основываться на анализе рисков, а план действий должен корректно учитывать расставленные приоритеты рисков. Начинать построение комплексной системы ИБ необходимо с внедрения базовых компонент защиты, таких как антивирусы, межсетевые экраны и т. д., постепенно переходя к более интеллектуальным и сложным технологиям и заканчивая средствами, позволяющими реализовать централизованное управление и мониторинг безопасности всей ИТ-инфраструктуры.

Причем необходимо помнить, что риски могут изменяться, поэтому план действий должен периодически пересматриваться и корректироваться.

Важно отметить, что итерационное развитие технической составляющей комплексной системы ИБ должно быть синхронизировано с аналогичным развитием организационной составляющей процесса управления ИБ на предприятии, без эффективной работы которой внедренные средства и системы ИБ будут малоэффективны.

Константин Кузовкин, компания "Ай-Теко". Современная сервисная модель оказания услуг ИТ и ИБ позволяет реализовать проект создания системы обеспечения информационной безопасности поэтапно, внедряя сервис за сервисом, процесс за процессом. Желательно, чтобы услуги ИТ и ИБ предоставлялись одним сервис-провайдером (системным интегратором) на основе единого соглашения об уровне сервиса,

в котором для каждой ИТ-услуги должны быть определены требования по ИБ.

Вячеслав Статьев, компания "РНТ". Развитие любой автоматизированной системы происходит поэтапно, и внедрение средств защиты должно происходить в рамках этого процесса. Необходимо осуществлять равноценное развитие трех основных составляющих автоматизированной системы предприятия: информационной, телекоммуникационной и составляющей по безопасности. Их одновременное развитие и учет их взаимовлияния на архитектуру системы, технологии обработки и обмена информацией очень важны с точки зрения эффективности процесса создания и развития системы. В настоящий момент в большинстве случаев имеет место другая ситуация, при которой сначала создается информационная составляющая автоматизированной системы, а потом приглашают специалистов по безопасности, для того чтобы полноценно защитить уже существующую и сильно развитую систему.

– Целесообразно ли использовать средства защиты от разных производителей или лучше ориентироваться на продукцию одной компании? Следует ли при этом отдавать предпочтение признанным брендам, или менее известные компании-разработчики также заслуживают внимания?

Алексей Лукацкий, компания Cisco. В среде специалистов по информационной безопасности бытует мнение, что два средства защиты от разных производителей лучше, чем одно. Аргументация очевидна – вторая преграда станет дополнительным барьером на пути злоумышленника, прошедшего через первую линию обороны. Считается, что разные производители по-разному реализуют те или иные защитные механизмы, что и позволяет надеяться на более высокую защищенность корпоративной сети, использующей два средства защиты вместо одного. Однако, на самом деле, две различные платформы для системы защиты несут с собой гораздо больше проблем, чем преимуществ.

Возьмем, к примеру, межсетевые экраны. По статистике, 99 % всех проникновений через эти, одни из самых распространенных, средства защиты периметра связаны не с "дырами" в программном обеспечении, а с их некорректной конфигурацией. При использовании двух межсетевых экранов этот риск возрастает вдвое, так как вероятность сделать ошибку увеличивается. Уязвимости в межсетевых экранах достаточно быстро обнаруживаются и так же быстро устраняются – производители средств защиты уделяют этому немало сил и времени. А вот с неправильной конфигурацией приходится бороться только самому пользователю. И здесь все зависит только от его умения и квалификации.

Конечно, нельзя категорично утверждать, что применение двух различных средств защиты не повышает, а снижает защищенность сети. Уже давно существуют примеры реализации межсетевых экранов с подсистемами проверки согласованности задаваемых правил. Если, например, в одном месте вы разрешите использовать IP-телефонию, а в другом запретите, такие системы сразу просигнализируют вам об этом. Можно пойти еще дальше: не только проверять согласованность правил, по которым будут работать средства защиты, но и сами правила создавать в автоматическом режиме, исключающем вероятность какой-либо ошибки. И сделать для этого надо совсем немного – интегрировать межсетевые экраны с системами управления информационной безопасностью. Эти системы знают, какие ресурсы и где именно в корпоративной сети находятся, какие пользователи и с какими правами имеют к ним доступ; а также регулярно проводят инвентаризацию всех происходящих в сети изменений. Почему бы не добавить в них механизм автоматической генерации правил разграничения доступа? Достоинство данного решения в том, что такие правила могут создаваться как для средств сетевой безопасности (межсетевых экранов, систем обнаружения атак и т. п.), так и для систем, защищающих отдельные сервера и рабочие станции (хостовых систем предотвращения вторжений, систем защиты от НСД и т. п.).

Кстати, можно пойти и по промежуточному пути, а именно воспользоваться возможностями двух защитных систем различных производителей, объединив их в одном продукте с единым управлением, настройкой и обновлением. В таком направлении действуют многие производители антивирусов, интегрируя в свои решения сразу несколько движков, дополняющих друг друга. В зависимости от ресурсов производителя он может подключать к своему антивирусу до 7-8 движков. Парадокс ситуации в том, что на рынке есть антивирусные продукты, которые вообще не имеют собственных движков, зато грамотно используют чужие. Производители антивирусов были первыми, кто активно пошел по этому пути, но не единственными. Эстафету подхватили разработчики средств обнаружения и предотвращения атак, использующие в своих продуктах не только собственные движки, но и, например, бывшую еще совсем недавно бесплатной систему Snort.

Андрей Малакеев, компания "Корпоративные Информационные Системы". Нет такой компании, которая предлагала бы весь спектр решений, необходимый для полной реализации системы безопасности. Рано или поздно все равно встанет вопрос об интеграции различных решений в единое целое (например, головная компания покупает "дочку", в которой используются другие решения), и лучше об этом подумать заранее, разработать концепцию, в которой будут определены технологии и механизмы интеграции. Признанные бренды предпочтительнее с точки зрения стабильности продукта, менее крупные компании более динамичны и лучше реагируют на требования пользователей, с ними проще работать.

Наталья Базаренко, компания RRC. Да, действительно, существует два подхода к выбору решений: все решения от одного производителя или необязательно от одного. Вроде бы, если все продукты нашего решения от одного вендора, то они, по идее, должны наилучшим образом интегрироваться и взаимодействовать друг с другом – то есть такое решение выглядит более грамотным. С другой стороны, мы уже понимаем, что обеспечение безопасности – это многоаспектная задача,

и каждый из известных производителей какие-то решения делает лучше других (как правило, с этими продуктами он и вышел на рынок и получил признание), а какие-то – нет. С третьей стороны, ИТ-инфраструктура основана на стандартных технологиях, поэтому поддержка тех или иных стандартов и протоколов должна обеспечить совместимость различных решений. Думаю, что, учитывая вышесказанное, следует использовать наиболее передовые практики решения тех или иных задач, но не учитывать их дальнейшую интеграцию, то есть пренебрегать интересами развития собственного предприятия и его системы безопасности было бы недальновидно.

Константин Кузовкин, компания "Ай-Теко". Зависит от ситуации. При необходимом количестве средств ключевую сетевую инфраструктуру центрального офиса предприятия желательно выстраивать на оборудовании признанного бренда с встроенными штатными средствами обеспечения ИБ. Защиту периметра удаленных филиалов (особенно, если их много) можно строить и на базе аппаратно-программных продуктов менее известных компаний. Среди продуктов для создания функциональных подсистем ИБ (например, защиты от спама, антивирусной защиты, управления событиями безопасности) существует немало конкурентоспособных решений (каждое со своими преимуществами и недостатками).

Михаил Башлыков, компания КРОК. В случае внедрения технологий анализа, например антивирусных решений, целесообразно использовать продукты от разных вендоров, так как существует вероятность того, что производители антивирусных средств могут выпускать обновления своих баз с разной скоростью.

Для других технологий, например обеспечения сетевой безопасности, правильнее ориентироваться на одного вендора, особенно, если он предлагает комплексное решение для защиты от множества угроз.

В любом случае, ответ на данный вопрос должен основываться на учете специфики конкретного предприятия, поскольку, помимо анализа функционала средств защиты, необходимо еще иметь в виду нюансы интеграции выбранного решения в существующую ИТ-инфраструктуру.

Кирилл Керценбаум, компания Symantec. Я уже говорил о том, что в последнее время в отрасли наметилась определенная тенденция к специализации в разработке решений защиты, и не всегда одна компания-производитель способна предложить весь набор решений, требуемых для реализации широкого спектра задач построения систем ИБ. При выборе конкретного производителя важно понимать, что любое программное или программно-аппаратное решение по ИБ практически бесполезно, если вместе с ним производитель не предоставляет клиенту, в явном или неявном виде, сервис по анализу текущего состояния угроз и консолидированные данные в виде баз или уведомлений. Главное, что подобный сервис на высоком уровне могут оказывать лишь компании, давно существующие и известные на рынке, неплохой же продукт защиты могут написать многие, в том числе новые и небольшие производители; без подобной же экспертизы продукты ИБ могут остаться лишь красивой оболочкой.

Вячеслав Статьев, компания "РНТ". Как правильно было уже замечено, ни одна компания не предлагает полного набора средств защиты, которые требуются для создания комплексной системы обеспечения информационной безопасности. Поэтому все существующие системы ИБ имеют неоднородный характер. Основная проблема при этом состоит в совместимости компонент такой комплексной системы между собой и с компонентами информационной и телекоммуникационной составляющей автоматизированной системы. Поэтому имеет смысл говорить об отработанных типовых решениях на базе элементов разных производителей. Построение таких типовых решений является более предпочтительным, чем просто выбор между однотипными решениями двух производителей. В данном случае напрямую работает системный принцип субоптимальности, когда оптимизировать надо систему в целом, а не ее компоненты по отдельности.

Олег Гудилин, компания "Лаборатория Касперского". Если говорить о крупных компаниях, то едва ли продукция какого-то одного вендора может удовлетворить все их потребности в области ИБ. Если же речь идет о небольших компаниях и защите отдельных сегментов ИТ-инфраструктуры, то тут можно смело обойтись и решениями от одного поставщика.

Что касается менее известных компаний-разработчиков, то очевидным плюсом использования их продуктов является их низкая стоимость по сравнению с решениями от известных производителей. Но, к сожалению, часто компании, выбравшие малоизвестного поставщика, оказываются жертвами своего желания сэкономить – такие поставщики, как правило, не могут оказать должный уровень поддержки и послепродажного сервиса. В результате, итоговая стоимость владения (TCO) такими решениями превышает аналогичный показатель у известных вендоров. Кроме того, внедрение средств защиты призвано снижать риски, а использование решений неизвестных поставщиков, скорее, увеличивает их.

Сейчас в России наблюдается интересная тенденция. Раньше даже крупные российские компании подходили к защите информации фрагментарно, внедряя отдельные продукты для обеспечения ИБ и не имея при этом четкого плана и стратегии защиты. Исключение, пожалуй, составляли только банки и другие финансовые учреждения. Но на наших глазах ситуация меняется кардинальным образом – все больше предприятий разрабатывают комплексные концепции защиты информации, наблюдается тенденция перехода от решения частных проблем безопасности к комплексному подходу. В этих новых условиях заказчику требуется уже не разрозненный набор продуктов защиты, а многоуровневая, зачастую территориально распределенная система, имеющая гибкие возможности управления. Все больше внимания компании уделяют не текущей стоимости приобретаемого решения, а TCO. На первый план выходит стоимость поддержки и эксплуатации программных и программно-аппаратных комплексов. В результате, свой выбор специалисты останавливают на поставщиках, учитывающих российскую специфику, способных предложить комплексные, легко управляе-

мые решения, качественный и оперативный сервис и техническую поддержку.

– Ряд компаний-разработчиков в области сетевых технологий предлагают, с целью повышения уровня безопасности корпоративной системы, переход на специально разработанные сетевые платформы, что нередко требует полного изменения не только уже имеющейся ИТ-инфраструктуры предприятия, но и всей привычной технологии использования аппаратно-программных средств. Насколько это оправданно, и можно ли оценить целесообразность и стоимость такого перехода?

Дмитрий Шепелявый, компания Oracle. Я со скептицизмом отношусь к системам защиты, требующим существенного изменения ИТ-структуры. Все-таки информационная безопасность – вторичная по отношению к ИТ вещь. Такой подход может быть целесообразен только в том случае, если защищаемая информация настолько критична, что иными средствами адекватного уровня защиты не добиться.

Алексей Лукацкий, компания Cisco. Если речь действительно идет о полной смене инфраструктуры, то это совершенно неоправданно, в том числе и с точки зрения безопасности. Новая платформа, новая инфраструктура, новая технология... Все это усложняет решение вопросов безопасности, требует переобучения сотрудников и т. д. Конечно, это не относится к случаю, когда просто пришла пора менять инфраструктуру по причине ее устаревания и, соответственно, невыполнения ею своих задач.

Наталья Базаренко, компания RRC. Целесообразность такого перехода должна рассматриваться, в первую очередь, с экономической точки зрения. Специализированные платформы, как правило, отличаются от неспециализированных тем, что часть необходимых настроек уже сделана производителем решения. Тогда переход на специализированные сетевые платформы имеет смысл при соответствующей ограниченности ресурсов и необходимости экономии при внедрении решения. Другая сторона вопроса – следует ли менять имеющееся решение (платформы) на другие, в том числе специализированные? Этот вопрос должен решаться, исходя из интересов дальнейшего развития бизнеса предприятия и, соответственно, его ИТ-инфраструктуры. И если очевидно, что через ограниченное время бизнес может затормозить свою работу из-за отсутствия необходимых технических ресурсов, то, безусловно, этот вопрос нужно рассматривать, и при выборе решения (в том числе платформ) постараться предусмотреть не только развитие инфраструктуры предприятия, но и технологий, которые развиваются в ИТ-сфере весьма стремительно.

Андрей Малакеев, компания "Корпоративные Информационные Системы". Как метод освоения средств – пойдет. Как путь эффективного решения задач обеспечения безопасности – весьма сомнительно. Нет смысла тратить огромные суммы на полную замену инфраструктуры, если достаточно суммы в тысячу раз меньшей для банального подкупа сотрудника.

Вячеслав Статьев, компания "РНТ". Любая специализированная и ориентированная на конкретное применение разработка потенциально является более предпочтительной там, где требуется высокая степень защищенности. Однако стоимость такой разработки, тестирования ее функционала, дальнейшего сопровождения многократно превышает стоимость решения, когда берется промышленное изделие внешнего производителя. Поэтому в данном вопросе все определяется желанием заказчика иметь уникальную разработку, которая может функционировать только в его интересах, и готовностью ее финансировать в значительных объемах.

Константин Кузовкин, компания "Ай-Теко". Переход на новую сетевую инфраструктуру – это очень болезненный для предприятия процесс, который связан с риском недоступности информационных ресурсов в течение определенного периода времени. Для обоснования такого перехода необходимо провести текущий анализ угроз и уязвимостей, а также оценку рисков и, в случае положительного решения, – продумать четкую организацию необходимых работ.

– Можно ли в беспроводных сетях достичь уровней защищенности, обеспечиваемых в традиционных сетях, или, с целью достижения максимальной защищенности, следует все-таки отказаться от беспроводных конфигураций?

Алексей Лукацкий, компания Cisco. Можно. Решения по безопасности беспроводных сетей ни в чем не уступают, а иногда и превосходят защитные системы в традиционных сетях. Приведу только один пример. Есть беспроводные контроллеры, которые не только выполняют функции точки беспроводного доступа и включают в себя традиционные защитные технологии (МСЭ, IPS, VPN и другие), но и могут определить физическое местоположение нарушителей в радиусе до трех метров. Традиционные системы защиты сегодня на это неспособны.

Дмитрий Шепелявый, компания Oracle. На мой взгляд, текущее состояние стандартов безопасности для беспроводной инфраструктуры способно обеспечить необходимый уровень защиты беспроводных сетей. Другое дело, что их надо грамотно применять, потому что для беспроводных систем риски неправильной настройки параметров безопасности гораздо выше, чем для проводных, в силу большей доступности беспроводной инфраструктуры для злоумышленников.

Кирилл Керценбаум, компания Symantec. При грамотном построении беспроводных сетей возможно добиться даже большего уровня защищенности, чем в проводных сетях. Объясняется это тем, что к защите данных в этом случае компании относятся намного более серьезно, так как беспроводной трафик по умолчанию более уязвим, и шифрование на качественном уровне – это единственное средство его защиты. Также существуют специализированные программные и аппаратные решения, которые позволяют обеспечить требуемый уровень

защиты беспроводных сетей, используя при этом множество их преимуществ.

Константин Кузовкин, компания "Ай-Теко". Стандарты безопасности, которые применялись первоначально в беспроводных сетях (IEEE 802.11, WEP) имеют определенные недостатки. Протокол WEP (Wired Equivalent Privacy) использует статические ключи и не требует обязательной аутентификации пользователя, его код легко вскрывается. Радикальное решение – выделение беспроводных пользователей в отдельный сегмент внутренней сети, на выходе которого стоит VPN-шлюз, а на рабочей станции пользователя – VPN-клиент.

Тем не менее существует надежное решение по защите информации на канальном уровне на базе технологий EAP (Extensible Authentication Protocol) и TKIP (Temporal Key Integrity Protocol), которые улучшают протокол WEP, а также алгоритма шифрования AES, как альтернативы алгоритму RC4, используемому в WEP. Технология TKIP и шифрование AES являются компонентами нового стандарта IEEE 802.11i и стандартов Wi-Fi Protected Access (WPA и WPA2).

Протокол EAP поддерживает надежные схемы аутентификации с использованием Radius-сервера, динамические сессионные ключи и алгоритмы управления ими. Поэтому, если грамотно задействовать и настроить все штатные средства защиты для беспроводных сетей, то можно достичь уровня защищенности даже выше, чем в традиционных сетях.

Вячеслав Статьев, компания "РНТ". Беспроводные сети находятся в стадии развития, и через некоторое время, я думаю, их защищенность достигнет требуемого уровня; в противном случае они просто перестанут существовать. То есть, это вопрос времени. Однако уже сейчас можно их использовать при определенных условиях, имея при этом высокий уровень защищенности. Например, применяя технологии абонентского шифрования передаваемых сообщений, можно быть уверенным, что конфиденциальность такой передачи будет обеспечена. Другое дело, что такое решение может быть не совсем технологичным.

Как мне кажется, масштабы нашей страны создают объективные предпосылки для развития беспроводной связи.

– Какими вы видите будущие системы информационной безопасности?

Михаил Башлыков, компания КРОК. Будущие системы ИБ будут, по всей видимости, максимально унифицированы, стандартизированы, а также – с возможностью централизованного мониторинга и управления.

Дмитрий Шепелявый, компания Oracle. Это будут системы, построенные на основе открытых стандартов, обменивающиеся между собой информацией в реальном времени и реализующие единую политику безопасности. Мне кажется, что ближайшее будущее за концепцией Security as a service, когда системы защиты информации предоставляют соответствующие услуги прикладным системам на основании политики безопасности, единой для всего предприятия, на базе технологии SOA.

Кирилл Керценбаум, компания Symantec. На мой взгляд, в этой области продолжится работа по совершенствованию механизмов защиты, в первую очередь, технологий эвристического анализа. Также будет продолжаться процесс консолидации различного функционала в единых продуктах, особенно для защиты самых уязвимых элементов ИТ-инфраструктуры – компьютеров пользователей. То есть наибольшей популярностью будут пользоваться этакие "комбайны", которые будут позволять решать одновременно несколько задач, обеспечивая при этом более высокий уровень защиты. В то же время, должны продолжиться разработки механизмов более глубокой интеграции программных продуктов ИБ в аппаратные ресурсы, что также позволит более эффективно противостоять непрерывно совершенствующимся технологиям, которые используют авторы разнообразного вредоносного ПО.

Вячеслав Статьев, компания "РНТ". В определенный период своей профессиональной деятельности я интересовался проблематикой искусственных иммунных систем с позиций обеспечения информационной безопасности. Ознакомление с существующими системами навело на мысль о том, что цели, решаемые задачи, технологии обеспечения безопасности информации в автоматизированных системах очень хорошо коррелируются с моделью иммунной системы человека. Необходимо только переложить эту модель на другую предметную область. Изучение развивающихся в настоящий момент многоагентных технологий в области обеспечения ИБ только укрепляет в этой мысли. Поэтому очень вероятно, что развитие технологий ИБ будет осуществляться в направлении создания адаптивных, самообучающихся систем, по своим принципам и механизмам функционирования аналогичным иммунной системе человека.

Владимир Баланин, компания TopS BI. В ближайшее время наибольшее внимание будет уделяться системам защиты данных и так называемым решениям endpoint security. И, несмотря на то что развитие информационных технологий ускоряется с каждым годом, постоянно меняется картина рисков и угроз, растет и развивается арсенал средств "киберпреступности" и, соответственно, средств защиты, всегда неизменным остается один элемент – человеческие ресурсы. Поэтому можно предположить, что в дальнейшем системы безопасности будут незримо присутствовать на всех уровнях обработки информации, чтобы, "не мешая" работать, вместе с тем жестко контролировать деятельность сотрудников.

В данном Круглом столе мы сфокусировали обсуждение темы организации системы информационной безопасности на современном предприятии вокруг вопросов технического обеспечения корпоративной политики ИБ, оставив в стороне другие аспекты защиты, о каждом из которых нужно говорить отдельно и обстоятельно. В этой связи многие спикеры подчеркивали, что меры обеспечения ИТ-безопасности должны носить комплексный характер, при этом большинство проблем могут быть решены за счет грамотных организационно-управленческих решений.

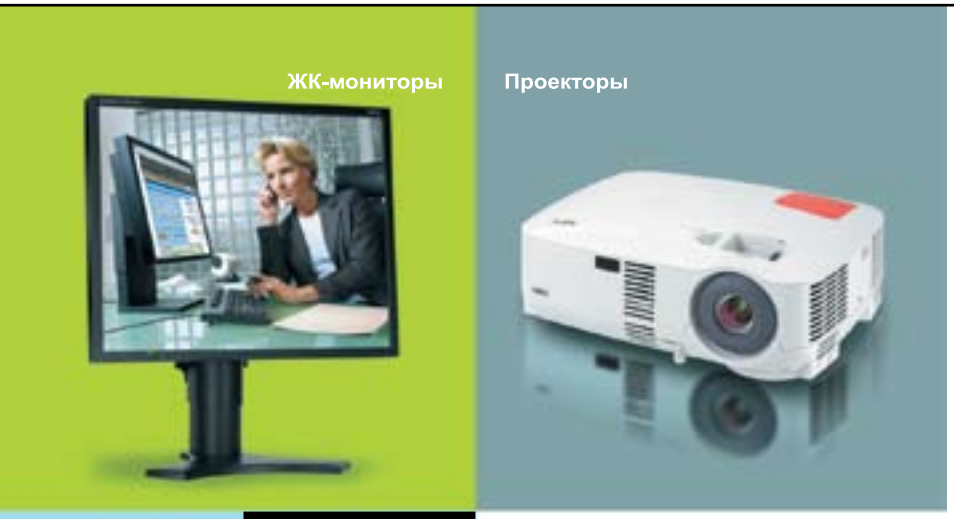
Среди участников обсуждения не было двух разных мнений в отношении того, что выборочная и бессистемная реализация защитных мероприятий не может обеспечить необходимого уровня ИТ-безопасности организации. Чтобы понять, какие меры защиты нужны предприятию, специалисты рекомендовали в первую очередь выстроить иерархическую структуру взаимосвязи угроз/рисков и определить наиболее уязвимые компоненты и процессы ИТ-инфраструктуры, после чего приступать к внедрению решений, призванных минимизировать ключевые риски. При этом, в отсутствие в настоящее время законченных технологических решений и универсальных методик по оценке рисков, необходима адаптация, собственными силами предприятий или с помощью специализированных компаний, общей методологии анализа и управления рисками под конкретное предприятие с учетом специфики его функционирования и бизнес-процессов. Поскольку основным критерием, которым руководствуются предприятия при выборе тех или иных средств построения системы ИБ является экономическая целесообразность, грамотно построенная модель управления рисками помогает потратить бюджетные средства предприятия с максимальной эффективностью.

Состоявшийся разговор не обошел стороной наметившуюся тенденцию к конвергенции средств защиты и управления ИТ, что характерно в особенности для крупных предприятий, заинтересованных более других в замене огромного, подчас хаотического количества отдельных продуктов ИБ комплексными интегрированными платформами. При этом отмечалось, что наибольший эффект от этого явления может быть достигнут при условии, что интеграционные процессы между ИТ и системами ИБ будут происходить не только на уровне программных продуктов, но и на уровне бизнес-процессов предприятия. Очевидно для большинства спикеров и то обстоятельство, что такая интеграция возможна только при наличии соответствующих систем централизованного управления, чье создание является в настоящее время важнейшей задачей в области ИТ, которой активно занимаются многие производители, но которая не имеет пока однозначного и эффективного решения. В связи с этим участвовавшие в беседе специалисты указали на особую актуальность, которую приобретает проблема унификации и стандартизации технологий управления средствами ИБ. Правда, обнадеживающим моментом здесь является то, что ее решение идет в направлении наследования лучших мировых стандартов.

Надеемся, что эти и другие обсуждавшиеся в данном Круглом столе вопросы, связанные с техническим обеспечением системы ИБ на современном предприятии, смогут помочь нашим читателям оценить состояние собственной корпоративной системы защиты информации и будут способствовать выработке взвешенных решений для создания эффективной, сбалансированной и защищенной ИТ-инфраструктуры своих организаций.

В заключение нашей беседы предлагаем читателям, перед которыми стоит задача повышения уровня защиты информационно-технологических ресурсов своих предприятий, обращаться за консультационной и практической помощью к экспертам, принявшим участие в настоящем обсуждении, адресовав свой запрос в редакцию или напрямую в заинтересовавшую компанию.

Круглый стол вела Елена Васильева



see more.
NEC Display Solutions

Видеть больше!

Empowered by Innovation NEC

NEC Display Solutions

Плазменные панели
и широкоформатные ЖК-мониторы
для общественных мест

Решения для каждого! Компания NEC Display Solutions выпускает широкую линейку средств визуализации изображений. От моделей начального уровня и заканчивая оборудованием для самых требовательных пользователей, все ЖК-мониторы, проекторы и плазменные панели отличаются современным дизайном, изображением высочайшего качества и широким набором дополнительных функций.

Представительство в Москве: Тел.: (495) 937-8410, Факс: (495) 937-8200

Реклама

RSI
Тел.: (495) 514-1419
www.rsi.ru

Легион
Тел.: (495) 601-9040
(812) 327-3129
www.legion.ru

DISTI GROUP
Тел.: (495) 380-2661
(495) 269-1776
www.disti.ru

Ланк
Тел.: (495) 730-2829
(812) 333-0111
www.lanck.ru

КомпьюЛинк
Тел.: (495) 956-3311
(495) 737-8866
www.compulink.ru

Trinity electronics
Тел.: (495) 737-8046
www.tri-el.ru

Русский Стиль
Тел.: (495) 737-5757
(495) 615-2057
www.rus.ru

www.nec-display-solutions.ru

INFOSECURITY RUSSIA 2008

infosecurity RUSSIA

7-9 октября 2008

Москва
Экспоцентр на Красной Пресне
Павильон №3

5-я международная специализированная выставка-конференция по информационной безопасности

Одновременно на одной площадке с Infosecurity Russia:

STORAGE EXPO

DOCUMATION

РАЗДЕЛЫ ВЫСТАВКИ

- Защита информации от несанкционированного доступа
- Системы мониторинга и фильтрации контента
- Межсетевые экраны
- VPN (виртуальные частные сети)
- Антивирусы
- Шифрование, PKI (инфраструктура открытых ключей)
- Технологии хранения и управления данными
- Меры по восстановлению информации после аварии, катастрофы и других чрезвычайных ситуаций (disaster recovery)
- Безопасность операционных систем / КИС
- Безопасность беспроводных систем
- Безопасность локальных и глобальных сетей
- Физическое обеспечение безопасности в информационных системах
- Маркеры доступа, смарт-карты
- Аутсорсинг безопасности (Managed Security Services)
- Сертификационные центры
- Биометрические системы
- Судебное разбирательство в компьютерной сфере

РЕСТЭК™

Reed Exhibitions

Дирекция выставки:
Санкт-Петербург,
Петрозаводская ул., д.12
Т.: (812) 320-80-98,
ф.: (812) 320-80-90
E-mail:itcom@restec.ru

www.infosecuritymoscow.com

Генеральный медиа-партнер: c-news Генеральный пресс-спонсор: Открытые системы Генеральный информационный обозреватель: SEC.RU КОРОТКИЙ ПУТЬ К ИНФОРМАЦИИ