Круглый стол

Технические аспекты построения системы информационной безопасности на промышленном предприятии

Перестройка российской экономики на передовой технологической основе, тесно связанная с использованием современных информационных и коммуникационных технологий, приобрела уже необратимый характер. В промышленных компаниях разного масштаба и уровня технологического развития производственные и бизнес-технологии непосредственным образом интегрированы в общую ИТ-инфраструктуру, которая играет все большую роль в повышении эффективности управления предприятием. Однако, с ростом значимости ИТ в промышленности, увеличением сложности и глобализацией информационных технологий резко возрастает и проблема защиты информационных и интеллектуальных ресурсов предприятий, которая стала сегодня одной из наиболее злободневных и актуальных. Обсудить технические аспекты проблемы информационной безопасности на промышленных предприятиях мы пригласили экспертов компаний ИТ-сектора, предлагающих свои решения в данной области.

В Круглом столе принимают участие:

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

– Каковы современные подходы к технической реализации разработанной на предприятии политики информационной безопасности? Какие программно-аппаратные средства и технологии входят в "контур" системы обеспечения ИБ?

Кирилл Керценбаум, компания Symantec. Нельзя однозначно определить какой-то перечень подходов к решению данной задачи. Как правило, каждая компания на основе разработанной самостоятельно или с привлечением сторонних экспертов концепции информационной безопасности на предприятии определяет для себя некие технические требования к подобной системе и обращается с ними к компетентным поставщикам или производителям решений. Можно, тем не менее, выделить два принципиальных варианта построения систем защиты: одновендорные и мультивендорные, другими словами, это варианты реализации системы на базе решений одного или нескольких производителей. Однако с учетом наметившейся в последнее время специализации производителей на определенных сегментах защиты второй подход сейчас более распространен. В "контуре" системы ИБ можно условно выделить несколько уровней защиты, которые реализуются с помощью набора программных или программно-аппаратных решений: защита внешнего периметра (Интернет и почтовые шлюзы передачи данных) и защита внутреннего периметра (сервера приложений и данных, персональные и мобильные компьютеры работников).

Андрей Малакеев, компания "Корпоративные Информационные Системы". На начальном этапе развития систем информационной безопасности основное внимание уделялось обеспечению защиты внутренних сетей от внешних угроз. Весьма модными тогда были истории про хакеров, проникающих в локальную сеть с вредоносными намерениями. Именно в то время и возник термин "контур информационной безопасности". Со временем стало очевидно, что внутренние пользователи намного опаснее хакеров. Необходимость "контура" – забора от этого, конечно, не пропала, но он перестал быть основным и единственным элементом системы ИТ-безопасности.

Если говорить о современных тенденциях в ИБ, то можно отметить стремление компаний сделать информационную безопасность частью общей системы безопасности предприятия, поскольку инциденты в области ИТ представляют собой, как правило, известные преступления, совершенные с помощью новых методов и технологий. Взять, например, кражу денежных средств. Раньше, до повсеместного внедрения ИТ, злоумышленники физически присваивали себе денежные знаки. Теперь, используя информационные технологии, они осуществляют электронный денежный перевод на нужный счет. И в том, и в другом случае совершается одно и то же преступное деяние – кража. Что это означает в контексте нашего разговора? Это означает, что при обеспечении безопасности в ИТ могут быть использованы методы, давно и успешно используемые в реальном мире, но реализованные на новых технических средствах. Примером может служить система регистрации действий пользователя в корпоративной сети в качестве аналога системы видеонаблюдения.

Дмитрий Шепелявый, компания Oracle. На мой взгляд, основным подходом к технической реализации политики безопасности должна быть возможность централизованного управления комплексом средств защиты информации на основании единой политики безопасности и открытых стандартов. Что касается программно-аппаратных средств, то они хорошо известны – это межсетевые экраны, IDS/IPS, антивирусы, Identity and Access Management, средства фильтрации контента, СКЗИ, СЗИ от НСД и т.д.

Наталья Базаренко, компания RRC. Основным критерием, которым руководствуются предприятия при выборе тех или иных средств построения системы информационной безопасности, является экономическая целесообразность этого исполнения (как и в остальных аспектах бизнеса), учитывающая стоимость владения системой защиты, а также соответствие результатов работы этой системы требованиям разработанной в организации политики ИБ.

Если говорить о конкретных типах технических средств, с помощью которых обеспечивается выполнение политики безопасности, по-прежнему актуальными остаются средства защиты периметра сети и рабочих станций – два наиболее распространенных типа, необходимость которых уже очевидна для администратора практически любой сети системы. В зависимости от ценности информации, циркулирующей в сети, может возникнуть также необходимость в средствах контроля и защиты сети внутри периметра. Эти аспекты защиты покрывают основную часть задач, связанных с реализацией политики безопасности. Нельзя, безусловно, умалять важность и таких направлений в ИБ, как идентификация и аутентификация пользователей. Полагаю, следует отдельно отметить тенденцию в развитии решений по безопасности, связанную с фокусированием производителей на защите данных, – возможно, это направление в скором времени можно будет выделить в отдельный класс средств защиты, но время покажет.

Большинство из названных типов средств защиты с точки зрения их функциональности существуют не первый год, изменения претерпело их техническое воплощение. В целом современные решения по информационной безопасности можно охарактеризовать как не просто технологичные, но и интеллектуальные. Сегодня с помощью технических средств мы боремся не только с "дырами" в ПО, но и с психологией злоумышленников.

Вячеслав Статьев, компания "РНТ". Грамотная реализация политики информационной безопасности современного промышленного предприятия предполагает применение комплексного подхода, в основе которого лежат инженерные, технические, программные, правовые, организационные, социальные меры и механизмы защиты. Эти меры направлены на обеспечение целостности и конфиденциальности информационных и телекоммуникационных ресурсов, а также их доступности для сотрудников предприятия в соответствии с их полномочиями. Политика информационной безопасности должна строиться применительно ко всему жизненному циклу изделий, включая и автоматизированную систему, обеспечивающую его информационную поддержку.

Основными направлениями мер по обеспечению политики ИБ предприятия являются:

- работа с персоналом;
- обеспечение безопасности речевой информации;
- обеспечение защиты интеллектуальной собственности;
- идентификация, проверка подлинности и контроль доступа на объект, в помещения, к ресурсам автоматизированной системы, реализация функциональных обязанностей пользователей, администрирование компьютерных сетей;

- защита АРМ пользователей, коммуникационных средств, серверов, внешних носителей информации, данных и программ в процессе обмена;
- обеспечение физической безопасности оборудования;
- обеспечение безопасности при разработке и сопровождении информационных подсистем;
- обеспечение безопасности при взаимодействии с внешними системами и сторонними организациями;
- защита информации от утечки по техническим каналам;
- организация контроля эффективности принимаемых мер защиты.

Михаил Башлыков, компания КРОК. Безусловно прав предыдущий спикер, что техническая реализация политики ИБ на современных промышленных предприятиях должна заключаться в построении комплексной системы информационной безопасности, охватывающей как технические, так и организационные меры защиты и контроля.

Если в этой комплексной системе отдельно выделить техническую часть, то в ее основе будут находиться программно-аппаратные средства, каждое из которых ориентировано на устранение определенных видов угроз: вирусов, утечки конфиденциальной информации, несанкционированного доступа по различным каналам связи и т.д.

Перечень угроз для каждого предприятия является уникальным, но, учитывая то, что в основе построения современных ИТ-инфраструктур лежат достаточно общеизвестные и распространенные технологии, большинство возникающих при этом угроз является типовыми. Поэтому можно выделить набор стандартных средств защиты, который определяет базовый "контур" комплексной системы ИБ, защищающий от наиболее серьезных и распространенных угроз. К таким средствам можно отнести антивирусные и антиспамовые решения, межсетевые экраны, системы контентной фильтрации сетевого трафика, средства аутентификации и контроля доступа, системы предотвращения сетевых атак, средства шифрования каналов связи.

Константин Кузовкин, компания "Ай-Теко". Политика информационной безопасности предприятия – это, совершенно верно, комплекс правил, процедур, практических приемов и руководящих принципов по защите информационных ресурсов предприятия. Технической реализацией политики является подсистема обеспечения информационной безопасности КИС.

Обычно в подсистему обеспечения ИБ входят следующие программно-аппаратные средства и технологии:

- межсетевого экранирования;
- обнаружения и предотвращения атак;
- защиты информации, передаваемой по каналам связи (VPN);
- управления учетными записями пользователей и контроля доступа;
- управления обновлениями программного обеспечения;
- резервного копирования и восстановления;
- централизованного управления средствами защиты;
- управления событиями информационной безопасности;
- защиты от спама;
- анализа контента (Web- и почтовых сообщений);
- инфраструктуры открытых ключей;
- строгой аутентификации;
- контроля деятельности сотрудников и др.

– Как зависит выбор конкретных средств информационной защиты от существующей на предприятии ИТ-инфраструктуры? Зависит ли он от таких факторов, как размер предприятия, специфика бизнес-процессов, уровень сложности ИТ-инфраструктуры и др.?

Михаил Башлыков, компания КРОК. Напрямую зависит. На выбор конкретных средств ИБ возможность их корректной и эффективной интеграции в существующую ИТ-инфраструктуру оказывает первостепенное влияние. Это подразумевает минимизацию возможного влияния механизмов защиты на пользователей и существующие бизнес-процессы. Необходимо отметить, что полностью исключить такое влияние часто даже не представляется возможным из-за специфики решения задач ИБ, предполагающих внедрение дополнительных ограничительных и контролирующих механизмов в ключевые места ИТ-инфраструктуры, с частью из которых пользователи вынуждены активно взаимодействовать.

В целом все перечисленные факторы имеют серьезное влияние на выбор средств ИБ. Так, размер предприятия, как правило, напрямую связан с размером ИТ-инфраструктуры, количеством пользователей, территориальной распределенностью и т.п. Чем больше предприятие, тем большие требования выдвигаются к производительности средств защиты и возможностям по их территориальному размещению и централизованному управлению. Специфика бизнес-процессов выдвигает свои требования к отказоустойчивости средств защиты и может накладывать ограничения на временные затраты пользователей, которые могут возникнуть после внедрения механизмов ИБ. Уровень сложности ИТ-инфраструктуры зависит, как правило, от ее размеров, архитектуры и степени неоднородности используемых средств и систем. Все это может являться источником дополнительных угроз и должно обязательно учитываться при проектировании комплексной системы ИБ и выборе соответствующих технологий защиты.

В идеале требования по обеспечению ИБ должны быть учтены еще на этапе проектирования и создания ИТ-инфраструктуры. Однако при необходимости внедрения

дополнительных и неучтенных ранее механизмов защиты в существующую инфраструктуру могут ставиться вопросы об их корректной интеграции и/или об архитектурных изменениях самой инфраструктуры ИТ.

Владимир Баланин, компания TopS BI. Разумеется, существующая инфраструктура оказывает влияние на выбор конкретных средств информационной безопасности, так как системы защиты информации, как правило, интегрируются в существующую ИТ-инфраструктуру либо являются ее частью. Например, при внедрении технологий NAC (Network Admission Control) можно столкнуться с определенными проблемами, если применяется оборудование разных производителей. Или, скажем, при внедрении систем управления идентификационными данными (Identity Management) и решений по однократной аутентификации и авторизации (Single Sign-On) выбор в пользу того или иного поставщика решения может быть мотивирован тем, что в его решении уже есть готовый интерфейс к применяемым на предприятии бизнес-приложениям. Размеры предприятия, несомненно, также имеют значение. Например, с точки зрения управления элементами комплексной системы ИБ может возникнуть необходимость делегировать некоторые функции управления службе технической поддержки или региональным администраторам, соответственно, данный функционал должен поддерживаться внедряемым решением.

Если говорить в данном контексте о влиянии специфики бизнес-процессов, то следует иметь в виду, что это влияние определяется одной из основных целей создания системы информационной безопасности, которая состоит в обеспечении непрерывного функционирования бизнес-процессов и минимизации возможного ущерба бизнесу путем предотвращения и снижения влияния инцидентов ИБ и т.д. Очевидно, что для каждого из бизнес-процессов существует свой набор угроз и уязвимостей, поэтому специфика бизнес-процессов через призму системы управления рисками определяет не только тип применяемых средств защиты, но и необходимость их применения.

Константин Кузовкин, компания "Айтеко". Это, действительно, так. Поскольку ИТ-инфраструктура предприятия состоит из нескольких основных уровней:

- физического (линии и аппаратура связи),
- сетевого (сетевое оборудование – маршрутизаторы, коммутаторы и т.д.),
- сетевых приложений и сервисов,
- операционных систем,
- систем управления базами данных,
- технологических процессов и приложений,
- бизнес-процессов предприятия,

то на каждом из этих уровней угрозы и их источники, методы и средства защиты, а также подходы к оценке их эффективности будут различными. Необходимо определить конкретные объекты защиты на каждом из уровней ИТ-инфраструктуры, разработать модели угроз и модели действий нарушителей для данного предприятия и провести анализ рисков. Только после этого можно сформулировать требования к подсистеме обеспечения информационной безопасности КИС и произвести в процессе проектирования подсистемы выбор конкретных средств защиты.

Обычно главной целью злоумышленника является получение контроля над информационными ресурсами на уровне бизнес-процессов. Поэтому определение конкретных мер защиты (в том числе и организационных) на этом уровне сильно зависит от специфики бизнес-процессов предприятия.

Андрей Малакеев, компания "Корпоративные Информационные Системы". Технологии обеспечения информационной безопасности должны не только соответствовать существующей ИТ-инфраструктуре, но и учитывать перспективы ее развития. Размер предприятия также предъявляет требования к масштабируемости выбранного решения, поскольку не секрет, что зачастую решения, успешно работающие в рамках небольшой локальной сети, оказываются абсолютно недееспособны в условиях большой, распределенной структуры ИТ.

Иван Мелехин, компания "Информзащита". Выбор конкретных средств защиты в первую очередь зависит от специфики бизнес-процессов и размеров предприятия. Ведь требования по защите формируются как раз на основе особенностей информационных активов, используемых в бизнес-процессах. Размеры предприятия, численность и организационно-штатная принадлежность эксплуатирующего данные средства персонала диктуют требования к способам управления средствами защиты. Существующая архитектура ИТ может определить выбор конкретного производителя средств защиты, обеспечивающего максимальную совместимость используемых средств, снижение затрат на обучение администрированию и поддержке.

Вячеслав Статьев, компания "РНТ". Безусловно, выбор средств и технологий защиты информации зависит от таких факторов, как размер и уровень сложности ИТ-инфраструктуры предприятия, специфика его бизнес-процессов, наличие квалифицированных кадров. Например, обеспечение целостности и доступности некоторого информационного ресурса для одного предприятия проще и дешевле обеспечивать на основе технологии резервного копирования/восстановления информации, в то время как для другого предприятия необходимо применять средства оперативного контроля и обнаружения негативных воздействий, которые потенциально могут привести к нарушению целостности и доступности информации. Существенным моментом здесь являются риски, ко-

торые предприятие готово принять, снизить, разделить, передать, трансформировать. Хотя, естественно, есть некоторые инвариантные решения, которые могут быть применены для любого предприятия.

Применение тех или иных средств определяется совокупностью объектов защиты, определенных в системе в качестве цели защиты. Например, для некоторых классов предприятий в качестве объекта защиты может быть определен персонал, выполняющий с применением информационных технологий производственные операции, которые являются критичными для бизнеса.

Кирилл Керценбаум, компания Symantec. Да, однозначно, все перечисленные в вопросе факторы находятся в прямой зависимости между собой. Во-первых, почти у всех производителей продуктов ИБ существует специальное разделение продуктов в зависимости от размеров и даже вида бизнеса компаний. Чем меньше компания, тем более интегрированные решения ИБ им нужны, – это удобнее и с точки зрения управления, и с точки зрения экономии ресурсов, человеческих и денежных. Соответственно, чем крупнее компания, чем критичнее системы, которые обслуживают бизнес, тем гранулярнее должны быть решения защиты.

Наталья Базаренко, компания RRC. Полагаю, что выбор средств и технологий защиты зависит от комплекса критериев и параметров, диктуемых реалиями предприятия. Чаще всего неважно, на каком оборудовании построена ИТ-инфраструктура, важно, что и как мы хотим защитить, а также то, как обеспечить ее соответствие политике безопасности, которая принята в организации. При выборе средств защиты в расчет идет множество параметров: структура сетевого окружения, ее сложность, количество администраторов безопасности на местах (включая их знания), размер предприятия, а точнее, производительность, которую должны поддерживать средства защиты. Кроме того, немаловажным фактором является популярность брэнда, а также стоимость не только приобретения, но и владения выработанным решением. То есть, кроме того, что решение должно обеспечивать необходимую функциональность, оно не должно стоить дороже, чем имеющиеся ресурсы предприятия (то есть, чем ценность и стоимость той информации, которую мы планируем защитить).

Это наиболее общий подход к выбору решений, когда речь идет об особо крупных предприятиях. Теперь возьмем другую крайность, когда предприятие не располагает ресурсами и возможностями позволить себе создание спланированной по всем правилам политики информационной безопасности. В этом случае все зависит от знаний и умений системного администратора. Тогда критериев будет два: первый – цена, второй – возможности сисадмина решить с помощью некоего недорогого продукта/продуктов (если это вообще возможно) текущую проблему или задачу. Но повторюсь, что упомянутые примеры представляют собой крайности, обозначающие границы, которые, как и во многом другом, определяют основную массу промежуточных вариантов.

Олег Гудилин, компания "Лаборатория Касперского". Выбор средств защиты полностью зависит от типа и степени угроз, с которыми приходится иметь дело предприятию. Например, предприятия финансового сектора гораздо чувствительнее к потере или краже конфиденциальной информации, так как их материальные и репутационные потери могут быть достаточно высокими. У производственных компаний или предприятий сферы торговли риски также высоки, но связаны они в большей степени с угрозой остановки бизнес-процессов, например, вследствие атак хакеров или саботажа персонала. Таким образом, чтобы понять, какие меры защиты нужны предприятию, необходимо прежде разработать модель рисков, определить наиболее чувствительные компоненты и процессы ИТ-инфраструктуры. После чего приступать к внедрению решений, призванных минимизировать ключевые риски. Тут стоит отметить, что ликвидировать все риски полностью не под силу никакой организации, но грамотно построенная модель управления рисками как раз помогает потратить бюджетные средства предприятия с максимальной эффективностью.

– В настоящее время в области разработок, касающихся технических аспектов обеспечения информационной безопасности, наблюдается тенденция к интеграции технологий защиты и инструментов управления ИТ. Чем это объясняется?

Михаил Башлыков, компания КРОК. Данная тенденция отражает общность вопросов и, соответственно, технологий поддержки ИТ-сервисов и обеспечения их безопасности. По сути, комплексная система ИБ – это одна из функциональных частей ИТ-архитектуры, поэтому существующее разделение технологий защиты и инструментов управления информационной инфраструктурой само по себе является несколько искусственным. Происходит просто закономерный процесс упорядочивания управления в рамках всей ИТ-инфраструктуры. Это явление наиболее явственно видно на примере крупных предприятий, для которых единственный способ не "потеряться" в хаосе существующих систем – это обеспечить централизованное управление ИТ, в том числе средствами и механизмами ее защиты.

Другое дело, что такая интеграция возможна только при наличии соответствующих систем централизованного управления, а также при большей унификации и стандартизации технологий управления средствами ИБ. В настоящее время все ведущие производители средств защиты предлагают подобные решения, использующие зачастую собственные протоколы межкомпонентного взаимодействия, что осложняет решение данной задачи в целом. Поэтому, такая интеграция – наиважнейшая задача в области ИТ, которая сейчас активно решается, но не имеет пока однозначного и эффективного ответа.

Существенные результаты в области интеграции достигнуты пока только на уровне функционала средств мониторинга, поскольку механизмы сбора событий с целью их последующего анализа достаточно унифицированы.

Кирилл Керценбаум, компания Symantec. Здесь можно выделить несколько основных причин: во-первых, существующая довольно напряженная ситуация с вредоносным кодом не оставляет производителям выбора перед необходимостью внедрения в своих продуктах все новых и новых механизмов защиты, при этом самым трудным остается соблюдение баланса риска и возможностей. Во-вторых, компании малого и среднего бизнеса, являющиеся неотъемлемой частью экономики, сталкиваясь с проблемами ИБ в не меньшей степени, чем крупный бизнес, часто не могут себе позволить внедрение и эксплуатацию большого количества разнородных и разрозненных систем защиты. И последнее: с учетом того, что системы ИБ, как правило, не являются основополагающими для бизнеса, компании часто не готовы тратить на них существенные средства и поэтому часто выбирают решения, наилучшим способом интегрирующиеся с существующей ИТ-инфраструктурой и тем самым позволяющие экономить на их обслуживании.

Владимир Баланин, компания TopS BI. Полагаю, что основной причиной интеграции является то, что большинство элементов системы ИБ, за некоторым исключением (например, средств защиты информации от утечки по естественным каналам), являются частью ИТ-инфраструктуры и, соответственно, находятся в зоне ответственности ИТ-департамента, который ими же и управляет. Еще следует заметить, что в применяемых на предприятиях стандартах по управлению ИТ (ITIL, COBIT) ИБ занимает не последнее место, поэтому в штатах ИТ-служб появляются специалисты по информационной безопасности. Вполне логично, что эти специалисты используют тот же инструментарий, что и департамент в целом.

Олег Гудилин, компания "Лаборатория Касперского". В первую очередь это связано с естественным желанием клиентов сократить издержки на поддержку своей ИТ-инфраструктуры. Поддержка разрозненных программных и программно-аппаратных решений – а их для защиты от различного типа угроз может быть достаточно много – очень ресурсоемкая задача. Поэтому наличие удобных встроенных средств администрирования или их интеграция с существующими инструментами управления сторонних производителей крайне важна для уменьшения стоимости владения (TCO) и возврата затраченных на покупку инвестиций (ROI). Кроме чисто коммерческих причин не стоит забывать о необходимости контроля над состоянием системы безопасности в рамках предприятия в целом.

Алексей Лукацкий, компания Cisco. Если посмотреть на задачи, решаемые ИТ- и ИБ-продуктами, то мы заметим, что они идентичны. На техническом уровне эти продукты должны обеспечить работоспособность и поддержку корпоративной инфраструктуры, а на уровне бизнеса – помочь в достижении бизнес-целей предприятия. А раз так, то противопоставлять безопасность и ИТ друг другу было бы неправильно. Наоборот, с целью снижения издержек и отказа от дублирования некоторых функций гораздо эффективнее и проще объединить ИТ и ИБ в рамках единого решения или продукта. И такие процессы сейчас активно идут. Например, всего несколько лет назад индустрия безопасности пришла к идее конвергенции схожих защитных функций в едином устройстве. Так родились многофункциональные системы отражения угроз (Unified Threat Management, UTM), которые объединяют в себе такие средства защиты, как межсетевой экран, систему построения VPN и отражения атак, антивирус и т.п. И действительно, каждая из этих систем выполняет одни и те же действия: получает IP-пакет, разбирает его, проводит анализ и затем отправляет дальше к месту назначения, иногда производя над ним какие-нибудь манипуляции (шифрование, перенаправление и т.д.). Разница только в методах анализа.

Но ведь и маршрутизатор, коммутатор или точка беспроводного доступа работает по тому же принципу – "принял, обработал, отправил". Почему же не интегрировать в рамках сетевого устройства еще и защитные функции. И такой шаг был сделан рядом сетевых производителей, которые сегодня предлагают маршрутизаторы с функциями межсетевого экрана, системы предотвращения атак, VPN, контроля URL и даже антивируса.

Аналогичная ситуация происходит и на системном уровне. Если раньше безопасность была "навесной", то сегодня нередки ситуации, когда производитель ОС, СУБД, ERP, Web-сервера и т.п. встраивает в свои решения достаточно мощные механизмы безопасности.

Разумеется, существуют и другие предпосылки к конвергенции. Например, усложнение и рост числа уязвимостей, устранение которых требует применения систем управления патчами и распределения программного обеспечения, которые находятся уже в ведении ИТ-подразделений, в то время как уязвимости и их поиск, как правило, являются прерогативой отделов информационной безопасности. И здесь никак не обойтись без координации деятельности двух подразделений, а то и использования единого инструментария. Среди других примеров можно привести:

- электронную почту, за функционирование которой отвечает ИТ, а за безопасность – ИБ;
- доступ к приложениям, предоставляемый ИТ, а определяемый ИБ;
- работу баз данных, которая организуется ИТ, а события безопасности от БД анализируются ИБ;
- конфигурацию сетевого оборудования или серверов и рабочих станций, реализуемую ИТ, а проверяемую ИБ на соответствие требованиям тех или иных стандартов (СТР-К, ISO 17799 и т.д.);
- встроенные средства безопасности беспроводных сетей, IP-телефонии, сетей хранения данных (SAN).

Вячеслав Статьев, компания "РНТ". Внедрение на предприятии современных ИТ-технологий предполагает, что в процессе эксплуатации созданной автоматизированной системы службы ее администрирования обеспечивают работоспособность системы с заданными характеристиками качества.

Основными характеристиками качества функционирования автоматизированной системы являются полнота и достоверность предоставляемой информации, обеспечение требуемого уровня конфиденциальности и доступности информационных услуг, поддержание надежностных и тактико-технических характеристик функционирования системы на требуемом уровне.

С этой точки зрения технологии защиты информации и технологии управления функционированием системы имеют одну общую цель – обеспечение требуемого уровня качества функционирования системы. Достижение этой цели предполагает решение целого ряда многофакторных задач управления, в рамках которых в большом числе случаев бывает практически невозможно разделить проблемные вопросы, относящиеся к сфере защиты информации или к сфере управления функционированием современной системы.

Различные объекты системы, протекающие в ней процессы и происходящие события имеют сложные взаимосвязи, зависимости и корреляции. В связи с этим для принятия своевременного и адекватного возникшей ситуации решения необходим всесторонний, комплексный анализ как текущего состояния системы, так и истории возникновения этого состояния. В процессе этого анализа должна привлекаться разнородная информация, собираемая как средствами управления функционированием системы, так и средствами защиты информации.

– Очевидно, что для построения сбалансированной системы информационной безопасности этап анализа рисков в этой области является определяющим как в плане выбора адекватных мер защиты, так и с точки зрения оптимизации расходов. Какие существуют технологии анализа рисков в области ИБ и от каких характеристик конкретного предприятия зависит применение той или иной методики?

Михаил Башлыков, компания КРОК. Несомненно, только результаты тщательно проведенного анализа рисков дают возможность адекватного выбора мер и средств защиты. Риски могут оцениваться качественно и количественно. Качественная оценка рисков направлена на выявление существующих рисков и их ранжирование по значимости и вероятности возникновения экспертным путем. Количественная оценка уточняет качественные результаты и, помимо оценки вероятности возникновения, включает еще оценку величины ущерба. Таким образом, в результате количественного анализа каждому риску ставится в соответствие величина возможных финансовых потерь в случае его реализации, что может служить в качестве обоснования необходимости внедрения соответствующих защитных мер и/или оценки необходимых бюджетных средств для их реализации.

Очевидно, что количественный способ оценки рисков значительно более сложный и дорогостоящий, поэтому его применение оправдано только в крупных и некоторых средних компаниях. Для малых предприятий зачастую может быть достаточно качественной оценки.

Дмитрий Шепелявый, компания Oracle. Какой метод оценки рисков ИБ выбрать, зависит от того, насколько точно можно рассчитать стоимость ИТ-активов, оценить вероятность реализации угрозы и степень уязвимости ИТ-системы к данной угрозе. Если эти данные более-менее точны (например, получены на основе изучения большого количества схожих угроз и инцидентов), то целесообразно использовать количественный анализ. В противном случае – качественный.

Вячеслав Статьев, компания "РНТ". В настоящее время мы вообще говорим о риск-ориентированном подходе при создании системы информационной безопасности. С точки зрения поставленного вопроса хотелось бы отметить несколько моментов:

Во-первых, большинство современных методик анализа рисков в области информационной безопасности на уровне ИТ-инфраструктуры базируются либо на вероятностно-статистических методах, либо на экспертном оценивании, как правило, с применением методов нечеткой логики.

Во-вторых, понятие "риск" имеет относительный характер и тесным образом связано с другим понятием – угрозой нарушения чего-либо. Поясню свою мысль на примере информационного фонда предприятия. С точки зрения администратора этого фонда существует угроза нарушения доступности и целостности информации, а с точки зрения пользователя-аналитика этого фонда речь идет об информационном риске, так как в случае несвоевременно полученной или недостоверной информации им может быть некорректно проведен анализ текущей проблемной ситуации.

В-третьих, при анализе рисков необходимо выстраивать иерархическую структуру взаимосвязи угроз/рисков в рамках ИТ-инфраструктуры предприятия, начиная с ее самых нижних уровней и доходя для прикладных рисков на уровне бизнес-процессов. Современные автоматизированные системы должны включать в себя средства, которые диагностировали бы степень влияния негативных событий, происходящих в автоматизированной системе, на реализацию требуемой бизнес-логики.

Андрей Малакеев, компания "Корпоративные Информационные Системы". Анализ рисков – это не этап, а постоянно выполняемая задача. Окружающий мир находится в постоянном развитии, изменении, и для того чтобы, как минимум, оставаться на достигнутом уровне, требуется также постоянно развиваться. Необходимо внедрять новые технологии, модернизировать бизнес-процессы и, соответственно, поддерживающую их ИТ-инфраструктуру. А любое изменение структуры ИТ (в крупных компаниях оно происходит постоянно), любое изменение в бизнес-процессах ведет к изменению значений рисков. Технологии оценки

рисков пока еще находятся в стадии развития, и говорить о каких-либо готовых технологических решениях пока рано. Есть системы, позволяющие реализовать тот или иной элемент общей задачи оценки риска, но законченное решение пока отсутствует.

Владимир Баланин, компания TopS BI. Существует множество методик по управлению рисками, например, OCTAVE, CRAMM, MAGERIT и др. Поэтому, наверное, не стоит говорить, что от каких-либо характеристик конкретного предприятия зависит выбор той или иной из методик. Главное для компании – это получить эффективный инструмент управления ИБ на основе анализа рисками. Выбор же методики может быть основан, например, на изучении лучших практик в конкретной отрасли либо на знаниях собственных специалистов по информационной безопасности, либо на доверии к организации, предоставляющей услугу по внедрению системы управления рисками. А вот уже на этапе внедрения методика адаптируется под потребности предприятия и/или дополняется средствами автоматизации ("Гриф", RiskWatch, Proteus, "Кондор", CRAMM, Cobra и т.п.), чтобы стать эффективным инструментом, которым смогут пользоваться собственные специалисты предприятия.

Андрей Суханов, компания "Информзащита". Действительно, основной целью проведения анализа рисков является выбор адекватных мер по обеспечению информационной безопасности, оптимальных по соотношению стоимость/уровень защиты. Выполнение проекта по анализу рисков предполагает необходимость решения нескольких достаточно трудоемких и важных задач. Первая из них – выбор методики анализа рисков.

Методики анализа рисков классифицируются в зависимости от того, какие методы оценки в них используются – количественные или качественные.

Применение качественных методов анализа рисков позволяет ранжировать угрозы и значимость их реализации для предприятия друг относительно друга. Оценка ущерба и вероятности риска при этом осуществляется приблизительно и может определяться на основании экспертного мнения исполнителей. Результатом проведения анализа рисков при помощи качественных методов является определение приоритетов по обеспечению информационной безопасности на предприятии.

Методики, использующие качественные методы оценки, рекомендуется применять в следующих случаях: анализ рисков информационной безопасности проводится на предприятии впервые; на предприятии отсутствует служба управления рисками; высшее руководство не использует анализ рисков в качестве механизма управления или хочет посмотреть на результаты пилотного проекта. В результате проведения анализа рисков могут быть обнаружены наиболее проблемные области в обеспечении информационной безопасности, для которых будет целесообразно провести более детальный анализ рисков по методике, использующей количественные методы оценки.

Применение количественных методов позволяет оценить риски в абсолютном денежном эквиваленте. Но для этого, во-первых, необходимо, чтобы на предприятии существовала развитая система управления рисками, в рамках которой разработаны методики определения операционных потерь. Во-вторых, оценка вероятности риска требует наличия обширной базы по инцидентам ИБ. В-третьих, не все потери выражаются в количественном эквиваленте. Примером тому может служить репутационный ущерб, привязка к денежной шкале по которому может быть задана только соответствующим подразделением предприятия, например PR-службой. Также при проведении количественного анализа рисков возникает вопрос, каким образом применение той или иной меры защиты влияет на вероятность и возможный размер ущерба от реализации риска. Способ решения данной задачи должен быть описан в методике анализа рисков.

Количественный анализ рисков позволяет решить задачу оптимизации расходов предприятия на меры по обеспечению информационной безопасности. Соответственно, проведение анализа рисков по количественной методике значительно дороже и сложней, чем по методике качественной. Это относится и к затраченному времени, и к стоимости инструментальных средств, и к необходимым для проведения работы профессиональным навыкам исполнителей.

Необходимо также учитывать, в каких масштабах проводится анализ рисков – для всего предприятия либо в рамках выделенных бизнес-процессов или структурных подразделений. Чем обширней область проведения данной работы, тем она более трудоемка, что дополнительно умножается на сложность применения методики, использующей количественные или качественные методы оценки рисков.

Константин Кузовкин, компания "Айтеко". Существует множество методик анализа рисков, как инструментальных (COBRA, CRAMM и др.), так и собственных корпоративных. В любой методике необходимо провести идентификацию информационных ресурсов, подлежащих защите, а также угроз и уязвимостей. Полнота такого списка зависит от уровня зрелости предприятия, специфики его деятельности и ряда факторов организационного порядка. Практика показывает, что невозможно предложить универсальную методику для всех предприятий. Необходима адаптация общих методик анализа и управления рисками под конкретное предприятие с учетом специфики его функционирования и бизнес-процессов. При этом большое значение имеет архитектура КИС, технологии обращения с информацией, составляющей коммерческую тайну предприятия.

Круглый стол вела Елена Васильева

Продолжение следует