

“Интерес организации к ИБ усиливается с каждым годом”

ЕЛЕНА ГОРЕТКИНА

Трудно найти другую область развития ИТ, которая развивается так динамично, как информационная безопасность (ИБ). С появлением новых технологий возрастает потребность в защите информации, в ответе на вопросы разработки новых законов. Как уследить за этим потоком? Решить данную проблему позволяют специализированные конференции, на которых пользователи встречаются с представителями регулирующих органов и компаний-вендоров. Одним из таких мероприятий является ежегодная всероссийская конференция “Информационная безопасность. Региональные аспекты. InfoBEREГ”, которая в нынешнем году проводится уже десятый раз. О ее особенностях и о ситуации в области ИБ рассказывает Юрий Малинин, ректор Академии Информационных Систем.

ИНТЕРВЬЮ



Юрий Малинин

пасности приобретают еще большую актуальность.

РС Week: Как развивалась тематика конференции на протяжении этих лет? Ю. М.: Мы внимательно следим за происходящими изменениями.

Например, пять лет назад был принят закон о защите персональных данных, во каждый год с его реализацией происходил какой-то новый поворот. Будем его обсуждать и в этом году, но теперь на первое место вышла тема безопасности в информационном обществе, связанная с реализацией государственной программы “Информационное общество”. Мы решили уделить этой теме особое внимание, потому что при принятии решений и утверждении документов, связанных с построением государственных информационных систем, вопросы информационной безопасности рассматриваются недостаточно. Однако в ходе реализации таких проектов возникает масса проблем, например в области межведомственного документооборота, защиты каналов связи, обработки данных.

Кроме того, в последнее время в конференции принимает участие больше представителей бизнеса, поэтому акцентировать основное внимание уделялось вопросам структуры, то сейчас фокус сместился в сторону интеллектуальной и ИТ-сферы. Что касается технологий, то на первых конференциях мы обсуждали вопросы обеспечения безопасности при построении распределенных корпоративных сетей, защиты периметра локальных сетей. Далее актуальными становились темы защиты от внутренних угроз и другие темы. Сейчас в связи с ростом популярности облачных вычислений будем рассматривать методы и технологии обеспечения ИБ в облаках. Ей будет посвящена целая секция, в том числе будут обсуждаться вопросы создания безопасного госсектора, разработки регуляторных органов, задавать вопросы и получать информацию из первых рук.

Сейчас, спустя десять лет, ситуация в регионах кардинально изменилась, новым ходом идет информатизация, переходящая на новый уровень предоставления услуг и сервисов. Но цели конференции “InfoBEREГ” остаются прежними и приобретают новый виток развития. Справедливо будет отметить, что на курсах на развитие информационного общества, и вопросы информационной безо-

формационной безопасности на протяжении десяти лет?

Ю. М.: Интерес государственных и коммерческих организаций к защите информации усиливается с каждым годом. Возможно, это связано с более глубоким проникновением ИТ во все сферы жизни. Но структура и бизнес по-разному относятся к ИБ.

Бизнес в первую очередь подходит к ИБ с точки зрения финансовых рисков. Особенно эти вопросы волнуют крупные компании. Малый и средний бизнес пока не очень осознает эту проблему. Но и крупные компании приходят к усилению регуляторных рисков, т. е. удовлетворять требованиям регуляторов. И тогда они начинают считать, что выгоднее — строить безопасную ИТ-инфраструктуру и внедрять средства защиты или содержать штат компетентных ИТ юристов и платить штрафы.

Что касается госструктур, за десять лет здесь произошли серьезные перемены. Ведь раньше в регионах вообще плохо понимали, зачем нужна ИБ, а теперь практически в каждом субъекте РФ созданы подразделения по ИТ и ИБ, которые решают вопросы информационной безопасности. Повышение внимания госструктур к защите информации сопровождается ростом бюджетов на ИБ.

РС Week: Стала ли обсуждение на конференции стимулом к законодательному регулированию и бизнеса при решении вопросов безопасности?

Ю. М.: Конференция является площадкой для обсуждения инициатив, которые затем рассматриваются законодательными и регулирующими органами. Например, несколько лет назад обсуждались вопросы стратегии развития информационного общества и предложения конференции вошли в соответствующую программу. На прошедших конференциях мы обсуждали также предложения регуляторов по нормативным документам, и результаты учли в экспертах, в работе этих документов. На конференции представляли регулирующих органов рассматривают о новых инициативах и разрабатывают новые правила.

РС Week: Какие вопросы безопасности преимущественно обсуждаются на конференции — общепрофильные или внутрисекторские?

Ю. М.: Конференция в основном сфокусирована на национальных вопросах. Но международный опыт тоже рассматривается, и зарубежные вендоры докладывают о новых технологических и мировых трендах. Кроме того, на конференции этого года мы хотим уделить внимание проблеме ИБ при трансграничном обмене, которая возникает в случае передачи документов из страны в страну по электронным каналам связи.

РС Week: Чем, по вашему мнению, отличаются ИБ-угрозы в 2011-м? Есть ли принципиальные изменения по сравнению с предыдущими годами? Ю. М.: Масштабы угроз постоянно растут и появляются их новые ви-

ды. В связи с массовым распространением ИТ увеличивается число любителей и профессионалов в этой области. Следовательно, растет и число тех, кто занимается непропорциональными действиями. Обострился проблема утечек персональных данных. Достаточно вспомнить случаи, например, когда приватная информация граждан попадает в Google и “Яндекс”. Важно, чтобы индивидуальное и корпоративные пользователи осознавали, к чему могут привести эти угрозы, а разработчики информационных систем и ПО уделяли больше внимания вопросам защиты.

В связи с массовым распространением и проникновением мобильных устройств в жизнь каждого человека особенно актуальной стала проблема защиты при мобильном доступе к корпоративным системам. Участились случаи мошенничества при дистанционном банковском обслуживании. Мы собираемся обсудить эти темы в следующем году. Но в целом громкие случаи утечек и взломов способствуют подъему рынка ИБ.

РС Week: Как вы оцениваете нынешнее состояние защищенности информации в России — в корпоративной среде, на федеральном и региональном уровнях? Что предприняты и органами власти должны еще сделать, чтобы улучшить ситуацию?

Ю. М.: Судя по последним событиям, информационная безопасность у нас не на самом высоком уровне, что и следовало ожидать. Раньше в государственных и коммерческих организациях не было ни бюджетов на ИБ, ни специалистов. Теперь на защиту информации выделяются средства, и многие федеральные и муниципальные организации имеют необходимые подотделенных специалистов.

Но многое еще предстоит сделать. Необходимо совершенствовать нормативную правовую базу. В этом году вышло много новых федеральных законов — № 63-ФЗ “Об электронной подписи”, № 99-ФЗ “О лицензировании отдельных видов деятельности”, № 161-ФЗ “О национальной платежной системе”, № 261-ФЗ “О внесении изменений в Федеральный закон «О персональных данных»”. Но, к сожалению, пока мало, а где то и нет позаконных нормативных актов, которые регламентируют реализацию этих законов. Что касается пользователей, то, к сожалению, у нас многие живут по принципу “пока гром не грянет...”. На рынке много средств защиты, но построить комплексную систему, учитывая всю известные и возможные уязвимости, просто. Важно найти баланс между стоимостью построения защищенных ИТ-систем и ценностью той информации, которую они защищают. Конечно, следует оценивать риски утраты данных и риски несоответствия требованиям регулятора, а затем принимать решения относительно средств и методов обеспечения безопасности.

И конечно, часто об этом говорят, не забывая о человеческом факторе. В любой организации помимо технических средств должна быть внедрена корпоративная политика безопасности, направленная на предотвращение утечек данных, а также четкий план расследования инцидентов: что и как делать, к кому обращаться. Такой комплекс мероприятий значительно снижает финансовые потери от угроз и позволяет внедрить технологичную защиту. Так что в первую очередь нужно выстроить правильную, а потом принимать решение о том, что и как закрывать техническими средствами.

Бизнес и госструктуры по-разному относятся к внедрению таких правил. Коммерческие компании финансово начинают от клиентов и поэтому начинают заботиться о безопасности бизнес-процессов, предоставляемых услуг гораздо раньше. Государственные организации традиционно зависимы от выделенного финансирования на обеспечение ИБ и здесь как раз регуляторные требования способствуют развитию ИБ. После принятия закона о персональных данных многие организации, и коммерческие, и государственные, стали серьезно задумываться о защите информации, потому как неисполнение закона влечет серьезные последствия.

Некоторые корпоративы произошли и на волне предстоящего финансового кризиса. Когда на предпринимателях началось сокращение ИТ-специалистов, увольнялись системные администраторы, которые в отместку нередко уносили с собой и пароли и базы, что приводило к инцидентам. В результате многие компании задумались об упреждающих работ по ИТ-системам и повысили внимание к вопросам защиты информации. Несмотря на режим сокращений и экономии, мы наблюдали увеличение бюджетов, выделяемых на безопасность в ряде компаний.

РС Week: Как обстоят дела с подготовкой кадров по ИБ? Есть ли потенциальные сдвиги?

Ю. М.: Сейчас вузы активно развивают эти направления. Но специалистов по ИБ все равно не хватает, так как спрос на них растет. Кроме того, уровень подготовки выпускников не всегда соответствует требованиям работодателей. На то есть ряд причин. Во-первых, устаревшая материально-техническая база. Но эта проблема сейчас решается разработчиками средств защиты, которые разворачивают в вузах свои лаборатории. К тому же многие вузы получили средства в рамках национального проекта “Образование” и направили их на оснащение своих лабораторий. Во-вторых, преподавательский состав хотя и имеет прочные фундаментальные знания, но зачастую слабо знаком с современными технологиями и нормативной базой, с лучшими международными практиками и стандартами.

Положительную роль в развитии системы подготовки специалистов по ИБ играет и учебно-методическое объединение вузов по информационной безопасности, которое тоже будет участвовать в конференции.

РС Week: Спасибо за беседу. ■