Информационная безопасность: поиск ответов путем диалога

Важность формирования национальной системы информационной безопасности невозможно переоценить. С 11 по 15 сентября в Сочи проходила VI всероссийская конференция «Обеспечение информационной безопасности. Региональные аспекты», организованная «Академией Информационных Систем». В работе конференции приняли участие представители министерств и федеральных ведомств, крупных бизнес-структур и отдельных предприятий, а также компаний – разработчиков средств защиты информации, профильных вузов и научно-исследовательских организаций. Целями данного мероприятия являлись: координация усилий министерств и федеральных ведомств, администраций субъектов Российской Федерации и организаций различных форм собственности в деле обеспечения информационной безопасности Российской Федерации, совершенствование правового регулирования в области информационной безопасности в РФ, оказание практической помощи государственным и коммерческим организациям в вопросах обеспечения информационной безопасности, а также обмен опытом ведущих специалистов.

В режиме прямого диалога с представителями регулирующих и контролирующих органов участники конференции обсуждали проблемы, касающиеся нормативно-правового регулирования, подготовки и внедрения отраслевых стандартов в области ИБ, вносили свои предложения.

Необходимость создания механизмов реализации уже принятых законов в области ИБ признали первоочередной задачей участники секции «Проблемные вопросы нормативного правового регулирования в области информационной безопасности».

Секцией «Практические вопросы обеспечения информационной безопасности государственных ведомств и коммерческих организаций Российской Федерации» было признано, что одним из наиболее актуальных направлений развития теории и практики ИБ следует считать разработку эффективных технических и организационных решений, технологий защиты от инсайдеров. На российском рынке появился ряд продуктов, использование которых способствует решению актуальных практических вопросов обеспечения ИБ.

Впервые в этом году проводилась секция «Стандарты ИБ в банковской сфере». Своим опытом внедрения Стандарта Банка России поделились П. В. Гениевский, исполнительный директор ЗАО «Метробанк», и А. Н. Велигура, заместитель генерального директора компании «АНДЭК».

В работе конференции приняли участие представители Федерального агентства по промышленности (Роспром), где в настоящее время также ведутся работы по защите информации. В итоговом выступлении представитель Роспрома отметил, что опыт, полученный на конференции, заставляет по-новому взглянуть на проводимые в рамках ведомства мероприятия.

На секции «Проблемные вопросы подготовки специалистов в области технической защиты информации» обсуждались вопросы развития межведомственной системы подготовки кадров, совершенствования дополнительного образования, разработки квалификационных требований к специалистам, сотрудничества образовательных и бизнес-структур в области подготовки специалистов по защите информации, а также опыт различных вузов страны по дистанционному обучению на базе современных обучающих технологий.

Участники секции одобрили усилия ФСТЭК и ФСБ России по методическому руководству подготовкой кадров, высказали пожелание ускорить внедрение в учебный процесс научно-технической продукции, создаваемой по заказу ФСТЭК, в частности типовых программ дополнительного образования, а также разработать квалификационные требования к руководителям и специалистам по защите информации.

Важнейшими задачами участники данной секции считают:

- кадровое обеспечение процесса подготовки специалистов в области защиты информации;
- создание системы аттестации специалистов в области защиты информации с периодическим повышением квалификации;
- создание научно-образовательных комплексов по изучению проблем ИБ в ведущих вузах и головных научно-исследовательских организациях в области ИБ.

Большой интерес вызвал «круглый стол» «Жизненный цикл сертификата соответствия требованиям безопасности информации на средства и системы информационных технологий», в ходе которого обсуждалось, что такое сертификат, чем отличаются друг от друга сертификации разных систем. Общее пожелание секции – рынку требуется некая инструкция по совмещению систем сертификации ФСТЭК и ФСБ. В настоящее время даже профессионалам трудно разъяснить соответствие этих систем, поскольку они сильно отличаются, хотя в целом решают одни и те же задачи.

Особенностью данной конференции является ее практическая и конструктивная направленность. Подводя итоги конференции, А. А. Стрельцов, директор департамента обеспечения безопасности информации и информационных технологий аппарата Совета Безопасности РФ, выразил озабоченность медленным развитием правового регулирования в области взаимодействия Российской Федерации и субъектов Федерации в вопросах обеспечения информационной безопасности. «Так, остается открытым вопрос о разделении полномочий между Российской Федерацией и субъектами Российской Федерации в области обеспечения информационной безопасности. В соответствии со ст. 71 Конституции РФ к ведению Российской Федерации отнесены «федеральные транспорт, пути сообщения, информация и связь». В соответствии со ст. 73 Конституции «вне пределов ведения Российской Федерации и полномочий Российской Федерации по предметам совместного ведения Российской Федерации и субъектов Российской Федерации субъекты Российской Федерации обладают всей полнотой государственной власти». Это означает, что информация, которая не является федеральной, относится к ведению субъектов Российской Федерации. В то же время остается неясным что это за информация, кто должен обеспечивать ее безопасность? На сегодняшний день данный вопрос не решен на концептуальном уровне». Фактически это следует расценивать, как приглашение к диалогу представителей субъектов РФ на следующей конференции.

Итак, до новых встреч в Сочи, теперь уже Олимпийском городе.

Юрий ЛАВРУХИН,
начальник Управления ФСТЭК России, член Исполкома АДЭ

В настоящее время во всех регионах Российской Федерации сложилось достаточно ясное понимание актуальности обеспечения информационной безопасности. Конечно, еще есть нерешенные вопросы, но серьезных проблем или преград на пути развития этого процесса в стране нет.

Основная задача сегодня – совершенствование нормативных документов, касающихся защиты ключевых систем информационной инфраструктуры, а также персональных данных. Сейчас идет формирование перспективного плана разработки нормативных документов с учетом накопленного опыта в ведомствах и отраслях.

Одна из важных целей настоящей конференции – организация связи с общественностью, а также с предприятиями, работающими на региональных рынках. Это помогает узнать «из первых рук», что в нормативных актах устарело, какие регуляторные механизмы нуждаются в корректировке, чего требуют современные реалии.

Нынешняя конференция наглядно показала, что практически во всех отраслях экономики уже подготовлены или введены в действие отраслевые системы защиты информации, и если даже где-то еще существует отставание, то движение, тем не менее, идет в верном направлении. Это заметно и по составу участников мероприятия – сотрудники госучреждений и ведомств, НИИ, разработчики систем ИБ, руководители и специалисты подразделений ИБ предприятий отраслей и т. д.

Необходимо отметить и то обстоятельство, что внедрение и поддержание на профессиональном уровне современных систем ИБ невозможно без соответствующих специалистов, недостаток которых ощущается, особенно в регионах. Понимая это обстоятельство, руководство ФСТЭК оказывает помощь в создании учебных центов по защите информации в регионах российской федерации.

Виктор ГАВРИЛОВ,
заместитель начальника Управления Центра безопасности связи ФСБ России

Рынок информационной безопасности развивается в нашей стране очень быстро, что порождает немало проблем. В частности, повсеместно не хватает профессиональных кадров. Во многих учебных заведениях обучение по специальности «Информационная безопасность» ведется недостаточно квалифицированно, выпускники плохо знают и существующую нормативную базу по безопасности информации, и сертифицированные средства защиты. Например, ряд типичных ошибок при разработке систем с использованием криптографических средств возникает вследствие недостаточного понимания того, как, собственно, функционируют механизмы криптографической защиты. При этом вместо полноценной подсистемы криптографической защиты информации заказчик может получить формально встроенные криптографические средства без учета адекватности их выбора, оценки правильности использования и анализа влияния программно-технического окружения системы на их специфические качества.

В условиях несовершенства законодательного регулирования следует признать весьма важной и полезной деятельность крупных коммерческих структур по разработке отраслевых стандартов информационной безопасности (Банк России, РАО «РЖД», «Газпром» и др.). Однако при этом не всегда учитываются существующие в стране положения регулирующих органов. Своевременное согласование положений отраслевых стандартов с регулирующими органами по вопросам, отнесенным к их компетенции, позволило бы избежать подобных ошибок.

Часть проблем возникает из-за отсутствия четких нормативов, которые обязывали бы заказчика в полном объеме проводить работу по защите конфиденциальной информации, не содержащей сведений, составляющих государственную тайну. При этом недостаточно четко определены и полномочия регулирующих органов.

В какой-то мере ситуацию исправляют поправки к законам «О техническом регулировании» и «О персональных данных». Однако они начнут полноценно работать лишь после принятия ряда подзаконных актов. Так, переходные статьи Закона «О персональных данных» позволяют использовать имеющиеся системы по старым правилам до 2010 г.

Однако и в перспективе вопросов с защитой информации в системах персональных данных останется очень много. Системы персональных данных могут содержать много другой информации ограниченного доступа, составляющей, например, врачебную, коммерческую, судебную тайну и т. д. Между тем, законодательные нормы, которые устанавливали бы обязательные требования по защите этих видов тайны, отсутствуют. Защита такой информации фактически является делом добровольным.

Поэтому задача регулирующих органов – ФСТЭК и ФСБ – предусмотреть в нормативных документах классификацию систем персональных данных по требованиям безопасности с учетом всех видов обрабатываемой информации ограниченного доступа, а не только персональных данных.

Владимир ГЕРАСИМЕНКО,
начальник ГНИИИ ПЗТИ ФСТЭК России

Вопросы правового регулирования сегодня важнее, чем вопросы о технических средствах обеспечения информационной безопасности. Отсутствие механизма, связывающего требования закона и применение технических средств, создает 80% проблем, обусловливающих недостаточную эффективность технической защиты информации. Хотелось бы, чтобы эти вопросы были решены как можно скорее, причем на федеральном уровне. Именно от того, насколько эффективно вопросы информационной безопасности будут отработаны на федеральном уровне, зависит то, как они будут решаться в регионах.

Одной из актуальных проблем на российском рынке информационной безопасности является недостаток квалифицированных кадров. Примерно за десять лет в стране появилась масса учебных центров со своими программами подготовки, но реальный уровень знаний выпускаемых ими специалистов явно недостаточен. Учебные курсы зачастую читаются людьми, не имеющими практического опыта работы с информационными системами. Сегодня необходимо ужесточить требования к таким вузам и учебным центрам с точки зрения их оснащения, программ обучения, чтобы процесс подготовки специалистов не был стихийным, а студенты получали качественное образование и становились квалифицированными специалистами.

Что касается собственно технологий, то интеллектуальный потенциал российских специалистов способен составить конкуренцию зарубежным решениям. Особенно это актуально в связи с тем, что представители иностранных компаний, разработчиков стандартов и продуктов проявляют интерес к совершенствованию процессов информационной безопасности на российском рынке. Но здесь уже начинают доминировать политические аспекты. Например, в начале процесса развития ИТ-технологий шли активные поставки компьютерных систем в университеты и крупные научные центры России. С одной стороны, речь шла о поднятии уровня оснащенности исследований, но с другой – это было изучение потенциала российской науки с последующим приглашением наиболее талантливых специалистов на Запад. Когда же встал вопрос о компьютеризации российских школ в рамках национального проекта, то поставить компьютерные классы в школы предложили тем же крупным зарубежным компаниям-поставщикам. Они отказали. Полагаю, причина одна – их пугает то, что если компьютеризация школ дойдет до глубинки, в области информационных технологий Россия сделает большой скачок вперед. А это уже и потенциал информационной безопасности страны. ■