

Редакция журнала планирует сделать тему информационной безопасности (ИБ) постоянной рубрикой. В этом номере ее открывает статья главы исполнительного комитета Ассоциации документальной электросвязи А. С. Кремера, год назад избранного председателем исследовательской комиссии МСЭ-Т по безопасности.

Направления деятельности ИК-17 включают и проблематику статей, вошедших в данную подборку, акцент в которой сделан на тему защиты персональных данных (ПДн) в информационных системах операторов связи. Вопрос тем более актуальный, что 1 января 2010 г. (пока!) определено как дата, когда все системы обработки ПДн должны соответствовать требованиям Федерального закона № 152 «О персональных данных», принятого в июне 2006 г. и вступившего в силу в 2007 г. На суд читателя выносятся результаты исследований в области ПДн, посвященных нормативно-правовому обеспечению закона, оценке угроз утечки ПДн, состоянию проектов в области обеспечения защиты информационных систем ПДн и т. д. Не секрет, что мнения о необходимости применения этих требований ко всем без исключения операторам ПДн высказываются самые противоположные: от полной ее бесполезности для субъектов ПДн до утверждений, что в результате операторы получат оптимальный по функционалу набор средств защиты.

Что не подвергается сомнению: закон требует существенной доработки. Опасения бизнес-структур, государственных ведомств, всех организаций, имеющих дело с ПДн, изложены в Рекомендациях парламентских слушаний — этот документ был разослан 20 октября 2009 г. Комитетом по безопасности Госдумы, где обсуждались актуальные вопросы развития и применения законодательства о защите прав граждан при обработке ПДн. Среди множества предложений прозвучало пожелание разделить даты введения санкций по этому закону на две составляющие: а) подготовку организационно-нормативной документации и общих мер защиты (это входит в сферу ответственности Роскомнадзора и не требует явной отсрочки) и б) исполнение требований ФСТЭК и ФСБ по мерам технической защиты, что связано со значительными инвестициями, а значит, санкции могут быть отсрочены на какое-то время.

Главное, однако, не дата начала проверок Роскомнадзора, а то, что ФЗ № 152 уже вступил в силу. Регулятор ведет активную деятельность в данном направлении, и операторам необходимо привести обработку ПДн в соответствие с требованиями закона. И это неплохая возможность выстроить надежную защиту своей информационной инфраструктуры.

УДК 004.7.056

СТАНДАРТИЗАЦИЯ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИЙ

А. С. Кремер, председатель исследовательской комиссии МСЭ-Т по безопасности, к. т. н.; kremer@rans.ru

Ключевые слова: безопасность электросвязи, информационная безопасность, сетевая безопасность, безопасность приложений, управление идентификацией, языки и методы описаний.

Введение. По представлению администрации связи России Всемирная ассамблея по стандартизации Международного союза электросвязи (МСЭ) в конце 2008 г. избрала председателем исследовательской комиссии по безопасности сектора стандартизации МСЭ (ИК 17 МСЭ-Т) представителя Российской Федерации. Срок полномочий охватывает четыре года: с 2009 по 2012 г. Учитывая актуальность стандартизации безопасности электросвязи, а также объединение в рамках МСЭ-Т администраций, организаций и бизнес-структур из более чем 190 стран, эффективное выполнение функций председателя комиссии, заключающихся в координации усилий по обеспечению информационной безопасности (ИБ) глобальных инфокоммуникационных сетей, в полной мере отвечает интересам нашей страны и содействует повышению ее международного авторитета.

ИК 17 МСЭ-Т — одна из десяти исследовательских комиссий сектора стандартизации. В 2001—2004 гг. она называлась «Сети передачи данных и телекоммуникационное программное обеспечение», в 2005—2008 гг. — «Безопасность, языки и телекоммуникационное программное обеспечение». В 2009 г. ИК 17 получила наименование «Безопасность». Два раза в год члены комиссии собираются на двухнедельные заседания, на которых обсуждаются и затем по одной из двух процедур: традиционной или альтернативной — утверждаются рекомендации МСЭ-Т.



Традиционная процедура утверждения применяется к рекомендациям, касающимся вопросов регулирования и безопасности жизнедеятельности. При этом члены комиссии имеют возможность представить свои замечания уже после того, как рекомендация была принята на заседании ИК, вплоть до ее следующего собрания. Процесс утверждения занимает до девяти месяцев.

Альтернативная процедура утверждения предусматривает представление замечаний в течение четырех недель после принятия рекомендации на заседании ИК. В этом случае процесс утверждения занимает до двух месяцев. Следует отметить, что по альтернативной схеме в МСЭ-Т утверждаются до 90 % рекомендаций.

Структура ИК 17 МСЭ-Т. На Всемирной ассамблее по стандартизации в 2008 г. ИК 17 была определена головной комиссией МСЭ-Т по безопасности телекоммуникаций, управлению идентификацией, а также по разработке языков и методов описаний. Другие девять комиссий МСЭ-Т тоже занимаются вопросами безопасности, относящимися к специфике их деятельности, согласовывая с ИК 17 планы своих исследований. ИК 17 готовит для МСЭ-Т предложения по координации работ, нацеленных на стандартизацию безопасности, взаимодействуя с другими ИК и секторами МСЭ, а также с различными организациями по стандартизации: ISO/IEC, ETSI, IETF, ATIS, OASIS, IEEE, Liberty Alliance и др.

В рамках ИК 17 образованы три рабочие группы: по сетевой и информационной безопасности, по безопасности приложений, по управлению идентификацией и языкам программирования.

Рабочая группа по сетевой и информационной безопасности (РГ 1) изучает пять вопросов:

- 1) проекты по исследованию безопасности;
- 2) архитектура и структура безопасности;
- 3) управление безопасностью;
- 4) кибербезопасность;
- 5) противодействие спаму.

К основным документам и рекомендациям, разрабатываемым в рамках РГ 1, относятся:

- словарь терминов и определений;
- путеводитель по стандартам безопасности;
- выявление пробелов в стандартизации безопасности;
- стратегия стандартизации, внедрения и оценки безопасности;
- архитектура внешних связей для управления безопасностью;
- базовый уровень информационной безопасности операторов связи;
- противодействие DDoS-атакам;
- обнаружение и противодействие botnet;
- противодействие распространению вредоносных кодов;
- безопасность информационных критических инфраструктур;
- обнаружение уязвимостей, оценка и минимизация рисков;
- комплексное обеспечение наблюдения, обнаружения и противодействия;
- формирование доказательной базы правонарушений.

Рабочая группа по безопасности приложений (РГ 2) изучает четыре вопроса:

- 1) аспекты безопасности повсеместных сенсорных сервисов;
- 2) безопасность прикладных сервисов;
- 3) безопасность сервисно-ориентированных архитектур;
- 4) телебиометрия.

К основным рекомендациям, разрабатываемым в рамках РГ 2, относятся:

- безопасность IPTV;
- защита сервисов и контента;
- безопасность мобильных устройств с несколькими сетевыми интерфейсами;
- безопасность мобильного банкинга;
- безопасность RFID;
- аутентификация с использованием одноразовых паролей;
- безопасность телебиометрии;
- безопасность веб-сервисов.

Рабочая группа по управлению идентификацией и языкам программирования (РГ 3) изучает шесть вопросов:

- 1) архитектура и механизмы управления идентификацией;
- 2) справочные службы, системы и сертификаты открытых ключей;
- 3) абстрактная синтаксическая нотация версии 1 (ASN.1), идентификаторы объектов (OID);
- 4) формальные языки и программное обеспечение для систем электросвязи;
- 5) языки и методики тестирования;
- 6) взаимодействие открытых систем.

К основным рекомендациям, разрабатываемым в рамках РГ 3, относятся:

- совместимость идентификации в глобальных сетях;
- персональная цифровая идентификация;
- директории и их безопасность;
- защита персональной информации;
- управление идентификацией (IdM) и безопасность систем IdM;
- присвоение идентификаторов объектам и безопасность инфраструктуры DNS;
- универсальный язык моделирования (UML);
- абстрактно-синтаксическая нотация версии 1 (ASN. 1);
- язык спецификаций и описаний (SDL);
- формальный язык разработки рекомендаций для обеспечения их тестируемости.

В 2009 г. состоялись два заседания ИК 17: с 11 по 20 февраля и с 16 по 25 сентября. В одном из них принял участие Генеральный секретарь МСЭ **Хамадун Туре**. В своем выступлении он дал высокую оценку деятельности ИК 17 МСЭ-Т, отметив, что комиссия «... должна формировать техническую политику и стратегию в области стандартизации безопасности и конфиденциальности при использовании ИКТ, содействовать координации усилий в этом направлении между всеми ИК МСЭ-Т, секторами МСЭ, а также при взаимодействии с другими организациями по стандартизации».

В 2010 г. в Женеве пройдут два заседания комиссии (с 7 по 16 апреля и с 8 по 17 декабря), а 6—7 декабря 2010 г. планируется провести семинар по безопасности.

Ближайшие задачи. Сегодня в ИК 17 МСЭ-Т особенно активно идет работа по включению в состав исследуемых направлений всех аспектов стандартизации безопасности телекоммуникаций, которые могут представлять интерес для операторских компаний и производителей оборудования. Среди таких перспективных направлений (пока они не входят в сферу деятельности комиссии) следует выделить:

- противодействие мошенничеству на сетях связи;
- использование криптографических средств в публичных сетях;
- законный перехват;
- безопасность автоматизированных систем расчетов и защита персональных данных в информационных системах операторов связи;
- унифицированное размещение признаков негативного контента для оказания услуг по его фильтрации;
- создание национальных центров управления устойчивым и безопасным функционированием публичных IP-сетей и координация деятельности таких центров.

С учетом нарастания в инфокоммуникационной отрасли процессов конвергенции связи, вещания и ИТ, ИК 17 рассматривает безопасность Интернета как неотъемлемую составную часть безопасности публичных IP-сетей. Все больше внимания комиссия уделяет безопасности DNS-инфраструктуры

и повышению роли операторов связи в обеспечении ее развития и безопасного функционирования.

Важнейшими задачами остаются совершенствование управления идентификацией в публичных сетях, стандартизация персональной цифровой идентификации, разработка предложений по обеспечению совместимости предлагаемых решений и выполнению операторами связи функций провайдеров услуг идентификации.

Для обеспечения безопасности глобальных сетей исключительно важно при присоединении сетей реализовать требования базового уровня безопасности. Такие требования уже сформулированы в рамках ИК 17, однако работа по их совершенствованию будет продолжена. Это новое направление стандартизации получило название «безопасность взаимодействия»: речь идет о межоператорском взаимодействии, а также о взаимодействии операторов связи с потребителями и силовыми структурами.

«Слабым звеном» в системе безопасности публичных сетей является любое оборудование, приложение или процедура, функционирование которых не определяется действующими стандартами безопасности или для которых подтверждение соответствия таким стандартам не проводилось. Очевидно, что подтверждение соответствия возможно лишь в том случае, если стандарт является тестируемым. Для обеспечения тестируемости рекомендаций МСЭ-Т в ИК 17 ведутся исследования по совершенствованию языка разработки тестируемых рекомендаций. Кроме того, продолжаются специальные исследования по введению программы подтверждения соответствия и маркировки оборудования, приложений и процедур, функционирующих в соответствии с рекомендациями МСЭ-Т.

Еще одним перспективным направлением деятельности ИК 17 является исследование бизнес-приложений стандартов безопасности. В рамках данного проекта изучаются лучшие практики реализации стандартов безопасности, разработанных как в МСЭ, так и в других организациях по стандартизации. Это позволит из множества стандартов безопасности выделить те, для которых можно сформулировать область применения и ожидаемые от их внедрения преимущества.

Заключение. Участие российских организаций в деятельности ИК 17 МСЭ-Т постоянно расширяется. Если в 2008 г. на заседания комиссии выезжали два-три эксперта, то в сентябре 2009 г. их было уже девять. Но важнее количественного показателя (который, несомненно, будет увеличиваться и дальше) то, что на заседания комиссии от имени администрации связи России представляются все более значимые вклады, в подготовке которых участвуют ведущие операторские компании. Для обсуждения и подготовки проектов таких вкладов в рамках общественно-государственного объединения «Ассоциация документальной электросвязи» создана специальная рабочая группа по стандартизации безопасности инфокоммуникационных сетей и систем.

Внося предложения по стандартизации безопасности в ведущую международную организацию, которой является МСЭ, мы повышаем авторитет и влияние России в мировом сообществе, изучаем зарубежный опыт решения задач, представляющих значительный интерес для российских инфокоммуникаций, содействуем выходу отечественных компаний на рынки развивающихся стран.

Получено 25.11.09

ПОЗДРАВЛЯЕМ ЮБИЛЯРА!



9 декабря 2009 года заместителю директора по науке ФГУП ЦНИИС Виктору Васильевичу Каледину исполнилось 70 лет.

К своему юбилею В. В. Каледин подошел, прожив интересную, иногда суровую, наполненную разнообразными событиями жизнь.

Виктор Васильевич родился в 1939 году в Тбилиси, где с золотой медалью окончил среднюю школу. После окончания с отличием Военного авиационного радиотехнического училища ВВС поступил в Военно-воздушную инженерную академию им. проф. Н. Е. Жуковского, которую с отличием закончил в 1969 году. Завершив учебу в академии, служил в разных частях и управлениях Минобороны, занимаясь развитием техники и методов

радиоэлектронной борьбы. В 80-х годах был командирован в Афганистан, где выполнял важные и ответственные задания.

В. В. Каледин закончил службу в Вооруженных Силах в 1992 году в должности начальника отдела Генерального штаба, в звании полковника. В общей сложности на этом поприще он посвятил служению Отечеству 34 года, стал классным специалистом в области радиотехники, приобрел опыт руководства решением сложных технических проблем и умение работать с людьми.

С 2000 года Виктор Васильевич работает в ЦНИИС, пройдя путь от директора научного центра до заместителя директора по науке. Занимаясь системно-сетевыми вопросами развития сетей связи, он вносит большой личный вклад в разработку и исследование методики использования и присвоения кодов на сетях подвижной связи стандарта GSM, в построение мультисервисных корпоративных сетей на основе перспективных технологий, обеспечение гармоничного взаимодействия поставщиков контента с операторами сетей при совместном оказании услуг связи и др.

Виктор Васильевич — активный участник семинаров и научных конференций, опытный и интересный докладчик, автор многих статей в научно-технических изданиях, в том числе и в нашем журнале. На его счету — авторские свидетельства на изобретения. Он награжден правительственными наградами: орденом «Красной Звезды» и 11-ю медалями.

Виктор Васильевич — прекрасный, высокообразованный специалист, умелый руководитель, чуткий, отзывчивый человек, приятный собеседник.

Редколлегия и редакция журнала «Электросвязь» сердечно поздравляют Виктора Васильевича с юбилеем и желают ему новых творческих успехов на ниве отечественной связи.