Международный союз электросвязи

ГОСУДАРСТВЕННОЕ АГЕНТСТВО ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ РЕСПУБЛИКИ БОЛГАРИИ

Региональный форум МСЭ по кибербезопасности 2008 года
София, Болгария

Документ RFS/2008/01-R
10 октября 2008 года
Оригинал: английский

ПРОЕКТ ОТЧЕТА О СОБРАНИИ

Региональный форум МСЭ по кибербезопасности для Европы и СНГ, прошедший в Софии, Болгария, 7–9 октября 2008 года[1]

Просьба присылать замечания по данному отчету о собрании по адресу: cybmail(at)itu.int

Цель настоящего отчета

1 Региональный форум МСЭ по кибербезопасности для Европы и Содружества Независимых Государств (СНГ) состоялся в Софии, Болгария, 7–9 октября 2008 года. Целью Форума, который провело Государственное агентство информационных технологий и связи (SAITC) Республики Болгарии, было выявление основных проблем, с которыми сталкиваются страны региона при разработке структур в области кибербезопасности и защиты особо важной информационной инфраструктуры (CIIP), изучение передового опыта, обмен информацией о деятельности в области развития, предпринимаемой МСЭ и другими организациями, и анализ роли различных субъектов в содействии развитию культуры кибербезопасности. На форуме также рассматривались инициативы регионального и глобального уровня по укреплению сотрудничества и координации между различными заинтересованными сторонами.

2 Форум, который явился одним из серии региональных мероприятий по вопросам кибербезопасности, проводимых Сектором развития электросвязи МСЭ (МСЭ-D), прошел в соответствии с Резолюцией 130 (Анталия, 2006 г.) Полномочной конференции МСЭ *Усиление роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий* и Дохинским планом действий Всемирной конференции по развитию электросвязи 2006 года, которым был создан Вопрос 22/1 для Исследовательской комиссии МСЭ-D *Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности*.
В мероприятии участвовали около 130 человек из 25 стран Европы и СНГ, а также из других регионов мира. Вся документация форума, включая окончательную повестку дня и все сделанные доклады, размещена на веб-сайте форума по адресу: www.itu.int/itu-d/cyb/events/2008/sofia/.
В настоящем отчете о собрании[2] вкратце отображен ход дискуссий, проходивших на протяжении трех дней работы Регионального форума МСЭ по кибербезопасности для Европы и СНГ, дается обзор сессий и докладов выступающих и приводятся согласованные на мероприятии решения. Участникам форума обеспечивался синхронный перевод на русский и английский языки.

Региональный форум МСЭ по кибербезопасности для Европы и Содружества Независимых Государств (СНГ), прошедший в Софии, Болгария, 7–9 октября 2008 года

3 В качестве базовой информации следует отметить, что в современных обществах наблюдается возрастающая зависимость от информационно-коммуникационных технологий (ИКТ), взаимодействующих друг с другом в глобальном масштабе. Страны все полнее осознают, что это порождает взаимозависимость, а также риски, которыми необходимо управлять на национальном, региональном и международном уровнях. Таким образом, укрепление кибербезопасности и защита имеющих ключевое значение информационных инфраструктур играют решающую роль в отношении

---

1 Веб-сайт Регионального форума МСЭ по кибербезопасности: http://www.itu.int/ITU-D/cyb/events/2008/sofia/.

2 Настоящий отчет о Форуме размещен по адресу: http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/sofia-cybersecurity-forum-report-oct-08.pdf.

безопасности и социально-экономического благосостояния всех стран. На национальном уровне это общая ответственность, требующая согласованных действий в отношении предотвращения инцидентов в киберпространстве, готовности к ним, реагирования на эти инциденты и восстановления после них со стороны органов государственного управления, частного сектора и граждан. На региональном и международном уровнях для этого требуется сотрудничество и координация с соответствующими партнерами. Таким образом, для разработки и внедрения национальных рамок в сфере кибербезопасности и защиты особо важной информационной инфраструктуры требуется всеобъемлющий, многодисциплинарный подход с участием многих заинтересованных сторон. На Региональном форуме по кибербезопасности обсуждался ряд ключевых элементов разработки таких политических и регламентарных рамок и предлагались конкретные меры для внедрения их в регионе.

Открытие собрания и приветственные речи

4 Региональный форум по кибербезопасности для Европы и СНГ открылся приветственным обращением[3] Пламена Вачкова, председателя Государственного агентства информационных технологий и связи (SAITC) Болгарии. От имени SAITC г-н Вачков приветствовал участников форума и подчеркнул, что данное мероприятие является важным шагом на пути создания потенциала кибербезопасности в Европе и СНГ. Г-н Вачков отметил, что проведение форума является выражением решимости SAITC и далее работать в сфере сетевой и информационной безопасности. В связи с этим он рассказал о ряде направлений деятельности агентства в этой области. Г-н Вачков также отметил постоянное участие SAITC в деятельности Европейского агентства по безопасности сетей и информации (ENISA), подчеркнув, что в результате активного сотрудничества с ENISA и венгерской группой CERT в Болгарии создается правительственная группа CERT. SAITC принимает меры для упрочения своего институционального потенциала в отношении информационной безопасности и разрабатывает национальную стратегию кибербезопасности, продолжил он.

5 Как наилучшим образом обеспечить кибербезопасность, поставил вопрос г-н Вачков. Поскольку большинство из нас проводит много времени в режиме он-лайн, а онлайновый виртуальный мир является отражением реального, как и преступники представляют собой неизбежную часть нашей социальной структуры, то неудивительно, что ими населен и виртуальный мир. Вместе с тем отметил он, если первоначально последствия этих киберпреступлений ощущались в основном в виртуальном мире, теперь жертвы киберпреступлений находятся в реальном мире и терпят значительные финансовые убытки или лишаются доверия. Логика проста, продолжил г-н Вачков: если есть киберпреступность, для борьбы с ней нужна кибербезопасность. Поэтому мы собрались на Региональный форум по кибербезопасности, сказал он, чтобы найти пути и способы повышения уровня кибербезопасности. Г-н Вачков завершил свои вступительные замечания, подчеркнув, что у Регионального форума по кибербезопасности масштабная повестка дня, что дает возможность организациям и странам региона обменяться опытом и работать для достижения общих целей в сфере кибербезопасности, способствуя созданию открытого для всех и безопасного информационного общества.

6 Сами Аль-Башир Аль-Моршид, Директор Бюро развития электросвязи Международного союза электросвязи (МСЭ)[4], также сделал ряд вступительных замечаний[5] от имени МСЭ. Он приветствовал участников форума и подчеркнул, что вопросы кибербезопасности представляют собой сложную смесь технологических, политических и культурных проблем. Г-н Аль-Башир напомнил участникам о ключевой роли, которую ИКТ играют в жизни людей, при том что число абонентов подвижной сотовой связи вскоре составит 4 миллиарда, а показатель проникновения подвижной связи по оценкам к концу года достигнет 61 процента. Доступ к ИКТ стал необходимым условием социально-экономического развития, а ИКТ помогают решить широкий круг повседневных проблем иногда неожиданными способами, сказал г-н Аль-Башир. Вместе с тем по мере развития новых технологий и расширения доступа к ИКТ возрастают и угрозы безопасности. Они носят глобальный характер – атаки в одной стране имеют последствия в другой, хотя лицо, производящее

---

3 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/saitc-opening-remarks-sofia-oct-08.pdf.

4 http://www.itu.int/ITU-D/dir/.

5 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/itu-opening-remarks-sofia-oct-08.pdf.

атаку, может физически находиться в третьей стране. Ввиду этого, продолжал он, для обеспечения безопасности киберпространства нам нужно применить глобальный подход и прийти ко взаимопониманию относительно того, как удовлетворить потребности всех стран, включая наименее развитые, развивающиеся и развитые страны. Мы сможем решить эти глобальные задачи, только действуя вместе для выработки стратегий и определения образцов передового опыта, отметил он.

7 МСЭ прокладывает путь к глобальному сотрудничеству, продолжил г-н Аль-Башир. На Всемирной встрече на высшем уровне по вопросам информационного общества МСЭ было поручено мировыми лидерами играть ведущую роль по Направлению деятельности С5, посвященному укреплению доверия и безопасности при использовании ИКТ. МСЭ силами трех своих Секторов вырабатывает глобальный, скоординированный и согласованный подход к обеспечению кибербезопасности посредством Глобальной программы кибербезопасности МСЭ – механизма международного сотрудничества, обеспечения синергии и координации усилий МСЭ. В рамках этих усилий Бюро развития электросвязи МСЭ предоставляет специальные знания и опыт посредством конкретной программы работы с инициативами и проектами, рассчитанными на удовлетворение потребностей Государств-Членов в повышении безопасности ИКТ. Эта программа работы включает организацию региональных форумов, подобного тому, который сейчас проходит в Болгарии, для создания в странах необходимого потенциала для эффективной борьбы с киберугрозами. Г-н Аль-Башир завершил свои вступительные замечания, заявив, что счастлив видеть всех присутствующих на форуме делегатов, и подчеркнув, что на нем встретились представители стран Европы и СНГ, региональных и международных организаций, чтобы обменяться опытом и совместно использовать образцы наилучшей практики для обеспечения безопасности, необходимой в киберпространстве для того, чтобы каждый мог пользоваться преимуществами информационного общества. Благодаря своим научным традициям, политическому опыту, накопленному в различные исторические периоды и исключительно богатой культуре Болгария обладает всем необходимым, чтобы сделать работу делегатов во время форума содержательной.

Заседание 1: На пути к интегрированному подходу к кибербезопасности и защите особо важной информационной инфраструктуры

8 Общепризнанна необходимость создания доверия и безопасности при использовании ИКТ, а также содействия обеспечению кибербезопасности и защите особо важных инфраструктур на национальных уровнях. Поскольку на национальном уровне государственный и частный секторы привносят свое понимание относительной важности вопросов, для формирования согласованного подхода некоторые страны создали институциональные структуры, тогда как другие страны использовали "облегченный", неинституциональный подход. Многие страны еще не разработали национальной стратегии в отношении кибербезопасности и CIIP. На первом заседании форума под председательством Валери Андрианавали, служащей отдела сетевой и информационной безопасности ГД "Информационное общество и медиасреда" Европейской комиссии, была представлена концепция национальных рамок для кибербезопасности и CIIP, обсуждалось, что сделано в этом отношении в Европе и СНГ на настоящий момент. Была также представлена постоянно ведущаяся в МСЭ работа по кибербезопасности, чтобы дать участникам собрания общее представление о проблемах, которые приходится решать, и вызовах, на которые приходится отвечать. Г-жа Андрианавали отметила, что цель проводимого мероприятия заключается в том, чтобы помочь странам лучше понять разнообразные обязанности, возлагаемые на различные заинтересованные стороны в отношении информационной безопасности, и содействовать странам в разработке национальных подходов к кибербезопасности.

9 Марк Саннер, ведущий аналитик по вопросам безопасности компании MessageLabs, в своем докладе, озаглавленном "Подготовка – меняющаяся обстановка в отношении угроз кибербезопасности"[6], поделился наблюдениями относительно того, как MessageLabs, будучи поставщиком комплексных услуг в сфере безопасности ИТ, видит собственное положение в интернете. Г-н Саннер отметил, что у MessageLabs есть центр обработки информации в интернете, и на основании 1,5 миллиарда ежедневных веб-запросов он дал представление о том, что его компания видит день ото дня, месяц от месяца, год от года. Г-н Саннер отметил, что обстановка в отношении угроз резко меняется и на смену вирусам приходят адресные "трояны" и атаки "фишинга",

6 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/sunner-threat-overview-sofia-oct-08.pdf.

имеющие точную социальную направленность. Существующая тенденция заключается в том, что хотя спам составляет по-прежнему значительную часть всех рассылаемых сообщений электронной почты, в целом объем спама за последние несколько недель сократился, и причина этого заключается в том, что был закрыт один из ПУИ в Соединенных Штатах, с которым давно были проблемы. Этим выступающий хотел показать, что существуют способы выведения из строя "управления войсками" и сокращения объема спама, доставляемого конечным пользователям. Он далее отметил, что каждое 131-е сообщение электронной почты по-прежнему содержит вирус какого-либо рода, а в августе 2008 года каждое 288-е сообщение электронной почты содержало фишинг. К концу 2007 года объем сообщений фишинга превысил объем вредоносных программных средств, и эти данные, как считает г-н Саннер, могут свидетельствовать о возможном направлении развития в этой области.
В заключение он отметил, что к концу 2008 года число вирусов снизится, но это означает, что "плохие парни" будут использовать больше url и гиперссылок, чем исполнимых модулей. Вместе с тем по сравнению с вирусами и спамом бот-сети растут быстрее.

10 Г-н Саннер привел конкретные примеры активности бот-сетей и отметил, что в Китае и Индии активность бот-сетей возрастает, что непосредственно связано с развертыванием в регионе широкополосной связи. Динамика развития среднего класса в Индии и Китае и развертывание широкополосной связи имеет четко выраженные последствия для всех нас. "История повторяется, – отметил он, – потому что наблюдается почти однозначное соответствие между числом подключений к широкополосной связи и объемом спама". Это уже наблюдалось в прошлом в Западной Европе и Соединенных Штатах и, вероятнее всего, произойдет в Индии и Китае в следующем году. К середине следующего (2009 г.) года в регионе значительно расширится доступ к широкополосной связи, и ввиду этого все ощутят увеличение потока спама, в особенности такие страны, как Япония, которые считают, что бóльшая часть спама поступает из Китая, заметил он. Г-н Саннер также привел информацию о ряде конкретных бот-сетей, на которые приходится значительная доля мирового спама. Упоминался и обсуждался также CAPTCHA – полностью автоматизированный публичный тест Тьюринга для различия компьютеров и людей. В отношении наблюдаемого увеличения частоты адресных атак г-н Саннер отметил, что хотя большинство основных атак направлены против всех, в 2005 году было только 1–2 адресных атаки в неделю, а сейчас их около 80 в день. В июне 2008 года произошло 540 атак за два часа, всех из них в документах, и все были направлены на названия профессий, людей с интересными тайнами, руководителей предприятий и т. п. Он считает, что источник этого – "черная" экономика, где продаются атаки DDOS и тому подобное. В некоторых регионах мира барьер для входа очень низок, а некоторые "поставщики" даже предлагают соглашения об уровне обслуживания, что точно отражает реальный мир и реальную экономику. Чтобы не создавать безопасных убежищ для такого рода деятельности, заключил он, необходимо ужесточить законодательство.

11 Александр Золотников, ответственный за информационную безопасность, ТрансТелеКом, Российская Федерация, представил доклад на тему "Киберпреступность в глобальных информационных сетях. Борьба с кибертерроризмом"[7] ТрансТелеКом, основным акционером которого являются Российские железные дороги, эксплуатирует и поддерживает крупнейшую волоконно-оптическую сеть в Российской Федерации – более 53 тыс. км кабеля, проложенного вдоль железнодорожных путей, и свыше 1 тыс. узлов доступа во всех регионах страны. С учетом широкомасштабного внедрения информационных технологий во всех слоях общества, в том числе особо важных инфраструктур, формирующих основу всех правительственных учреждений, в финансовой и банковской сферах, в областях транспорта, энергетики и общественной безопасности, обеспечение информационной безопасности стало одной из основных задач правительства, отметил он. Защита объектов особо важных информационных инфраструктур является серьезной задачей как для государства, так и для частных предприятий, которые являются владельцами этих инфраструктур как на национальном, так и на международном уровне.

12 Существующие в сетях проблемы, отметил он, являются проблемами компании, поскольку услуга предоставляется клиенту напрямую оператором. Ввиду этого роль и соответствующие обязанности оператора электросвязи в области кибербезопасности весьма важны, и ими не следует пренебрегать. В своем выступлении г-н Золотников рассказал о конкретных обязанностях оператора по созданию безопасных информационных сетей и сетей электросвязи. Он подчеркнул

---

7 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/zolotnikov-cyberfighting-sofia-oct-08.pdf.

необходимость того, чтобы каждый оператор внедрял системы эффективного мониторинга сетей и активно боролся с мошенничеством. Он далее разъяснил, что оператор должен взаимодействовать и делиться опытом с другими операторами, регулярно взаимодействовать с правоохранительными органами и спецслужбами, а также подчеркнул, что операторы должны активно участвовать в национальных и международных форумах, чтобы принимать участие в обсуждениях и узнавать, что другие делают в этой области.

13 Ведущая заседание Валери Андрианавали, служащая отдела сетевой и информационной безопасности ГД "Информационное общество и медиасреда" Европейской комиссии, сделала сообщение на тему "Безопасность и устойчивость в информационном обществе: к политике CIIP в ЕС"[8]. Г-жа Андрианавали начала сообщение с обзора существующих в Европейском союзе политики и законодательства, а также роли Европейской комиссии в разработке политики и законодательства в отношении CIIP. Среди представленных мер Стратегия для безопасного информационного общества 2006 года; политические инициативы по борьбе со спамом, шпионским программным обеспечением и вредоносным программным обеспечением, содействующие защите данных и борьбе с киберпреступностью; предложенный пакет по реформированию регламентарных рамок для электронной связи; создание Европейского агентства по безопасности сетей и информации (ENISA); и политическая инициатива по CIIP, которую предстоит принять в начале 2009 года в общих рамках Европейской программы по защите особо важных инфраструктур. Цель новой политической инициативы в отношении CIIP заключается в том, чтобы повысить степень готовности к CIIP и реагирование в этой области в ЕС, а также обеспечить наличие надлежащих и последовательных уровней мер по предупреждению, обнаружению, действиям в чрезвычайных ситуациях и восстановлению. Для достижения этих целей требуется углубить понимание и добиться ясности в отношении руководящих политических принципов, подчеркнула выступающая. Подход, применяемый для достижения целей политики, предусматривает расширение существующих национальных инициатив и инициатив частного сектора, привлечение соответствующих заинтересованных сторон из государственного и частного секторов и тесное сотрудничество с региональными и международными инициативами в этой области.

14 Г-жа Андрианавали далее подчеркнула необходимость сокращения разрывов в отношении национальной политики по CIIP в странах Европы и оказания помощи странам, менее развитым в этой области, с тем чтобы поднять все страны до единого уровня и укрепить сотрудничество и обмен информацией между странами. Также она отметила важность международного аспекта CIIP и необходимости укреплять сотрудничество по соответствующим глобальным вопросам, таким как безопасность и надежность интернета. Успешное осуществление новой политической инициативы станет значительным шагом вперед в реализации Стратегии Европейской комиссии для безопасного информационного общества, подчеркнула выступающая. Г-жа Андрианавали завершила свое выступление рассказом о ряде следующих планируемых в Европейском союзе мер в отношении CIIP. Уже подготовлен и начат ряд исследований в отношении новой политической инициативы, завершить которые планируется к концу первого квартала 2009 года. К их числу относятся исследования, целью которых является совершенствование понимания того, как различные секторы промышленности зависят от ИКТ. Уже проводится исследование по секторам финансов, энергетики и транспорта, и его результаты будут обнародованы в конце 2009 года. Также началось проведение анализа реализуемых в регионе инициатив. Г-жа Андрианавали далее подчеркнула, что цель Европейской комиссии – не дублировать работу, уже проводимую в государствах-членах, а наращивать синергию и оказывать помощь странам, менее развитым в этой области, с тем чтобы поднять все страны до единого уровня готовности. Цель заключается в принятии подробного плана действий по CIIP к первому кварталу 2009 года.

15 Марко Обисо, Советник Отдела приложений ИКТ и кибербезопасности Бюро развития электросвязи МСЭ (БРЭ), представил обзор по теме "Деятельность МСЭ-D в области кибербезопасности и защиты особо важных инфраструктур (CIIP)"[9]. Вначале он рассказал о деятельности МСЭ в области кибербезопасности в целом, отметив, что деятельность, связанная с кибербезопасностью, ведется во всех трех Секторах МСЭ. Сектор развития электросвязи, отметил он, находится на переднем крае деятельности МСЭ в различных регионах, тесно сотрудничая с

---

8 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/andrianavaly-CIIP-in-EU-sofia-oct-08.pdf.

9 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/obiso-overview-of-activities-sofia-oct-08.pdf.

партнерами по осуществлению проектов и инициатив. Подход с участием многих заинтересованных сторон необходим для всех видов деятельности МСЭ, продолжил он, в особенности в области кибербезопасности, поскольку относящиеся к ней задачи нельзя решать по отдельности. Г-н Обисо подчеркнул, что МСЭ решает проблемы, связанные с Направлением деятельности С5 ВВУИО, посвященным укреплению доверия и безопасности при использовании ИКТ, с помощью Глобальной программы кибербезопасности – инструмента, который МСЭ использует для объединения и согласования внутренней деятельности по кибербезопасности, проводимой во всех трех Секторах МСЭ, и для работы с внешними заинтересованными сторонами, организациями и экспертами, обеспечивая также выполнение рекомендаций на основе Глобальной программы.

16 Далее г-н Обисо рассказал о Программе работы МСЭ-D в области кибербезопасности для помощи развивающимся странам (2007–2009 г.)[10], приводя конкретные примеры работы, которую МСЭ проводит для помощи развивающимся странам в области кибербезопасности и CIIP. К числу проводимых и планируемых МСЭ инициатив в области кибербезопасности, упомянутых в выступлении, относятся: деятельность, связанная с выявлением передового опыта в применении национального подхода в области кибербезопасности и CIIP; национальный инструмент самооценки готовности в области кибербезопасности/CIIP; инструментарий для смягчения действия бот-сетей; публикации руководящих указаний в области кибербезопасности для развивающихся стран; международный обзор национального потенциала в области кибербезопасности/CSIRT; инструментарий по типовому законодательству, направленному против киберпреступности, для развивающихся стран; инструментарий по распространению культуры кибербезопасности, а также ряд планируемых региональных мероприятий по повышению осведомленности и созданию потенциала в области кибербезопасности и CIIP. Далее выступающий отметил, что в Программе работы излагается, как МСЭ практически может и планирует помочь странам в развитии потенциала в области кибербезопасности, предоставляя Государствам-Членам полезные ресурсы, справочные материалы и инструментарии по соответствующим вопросам, а также осуществляя ряд проектов в различных странах и регионах. Когда соответствующие инструментарии и справочные материалы будут доработаны, МСЭ-D собирается по различным каналам распространить их среди 191 Государства – Члена МСЭ.

17 Джозеф Ричардсон, консультант, Соединенные Штаты Америки, представил более подробный анализ "Подхода МСЭ к организации на национальном уровне деятельности в области кибербезопасности/CIIP и инструментарий МСЭ по самооценке в области безопасности"[11]. Г-н Ричардсон описал подход к организации на национальном уровне деятельности в области кибербезопасности/CIIP, который включает политические заявления, определяет цели и конкретные шаги по достижению этих целей, а также справочные и другие материалы по каждому отдельному шагу. Подчеркнув, что защита киберпространства необходима для национальной безопасности и экономического благосостояния, г-н Ричардсон далее привел конкретные примеры того, как страны могут начать разрабатывать национальную стратегию в области кибербезопасности. Важным шагом в этом направлении является проводимая МСЭ работа по составлению комплексного Национального инструментария МСЭ по самооценке в области безопасности/CIIP[12]. Этот инструмент может помочь правительствам изучить существующие национальные стратегии, процедуры, нормы, институты и другие элементы, необходимые для формулирования стратегий безопасности в постоянно меняющейся среде ИКТ. Он способен помочь правительствам лучше понять существующие системы, выявить имеющиеся пробелы, требующие особого внимания, и определить приоритетность национальных мер реагирования в области кибербезопасности.

18 Г-н Ричардсон разъяснил, что этот инструмент определяет темы и поднимает ряд вопросов, заслуживающих рассмотрения: какие меры были приняты на настоящее время, какие меры рассматриваются и каков статус этих мер? Г-н Ричардсон также отметил, что ни одна страна не начинает с нуля, когда речь идет об инициативах в области кибербезопасности, и что нет одного правильного ответа или подхода, поскольку у всех стран есть особые национальные потребности и обстоятельства. Также необходимо постоянно анализировать и пересматривать любой применяемый

---

10 http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

11 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/richardson-overview-of-approach-sofia-oct-08.pdf.

12 http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

подход, и столь же важно привлечь все заинтересованные стороны, в соответствии с их ролями, к разработке национальной стратегии. Страны, заинтересованные в проведении при содействии МСЭ национальной самооценки в области безопасности/CIIP, могут обратиться в Бюро развития электросвязи МСЭ по адресу: cybmail@itu.int.

Заседание 2: Содействие развитию культуры кибербезопасности

19 Доверие и безопасность при использовании информационно-коммуникационных технологий жизненно важны для построения открытого для всех, безопасного и глобального информационного общества. Непрерывные изменения в использовании ИКТ, систем и сетей предоставляют значительные преимущества, но также требуют гораздо большего внимания к кибербезопасности и защите особо важной инфраструктуры со стороны правительств, коммерческих предприятий, других организаций и отдельных пользователей, которые разрабатывают эти сети, владеют ими, предоставляют их, управляют ими, обслуживают и используют эти сети. Учитывая свойства, обеспечивающие взаимодействие ИКТ, содействовать настоящей кибербезопасности можно только при условии, что все соединенные заинтересованные стороны осознают существующие опасности и угрозы и то, как они могут защитить себя в онлайновом режиме. Правительства должны играть ведущую роль в формировании культуры кибербезопасности и в оказании поддержки усилиям других сторон, направленным на это. Кроме того, чрезвычайно важно региональное и международное сотрудничество для содействия развитию глобальной культуры кибербезопасности. На заседании 2, которое вела Джейнис Ричардсон, представитель организации European Schoolnet и координатор инициативы "Более безопасный интернет", подробнее рассматривались составные элементы, необходимые для успешного содействия развитию культуры кибербезопасности.

20 Кристин Санд, координатор по кибербезопасности, Отдел приложений ИКТ и кибербезопасности, Сектор развития МСЭ (МСЭ-D), в своем докладе "Содействие развитию культуры кибербезопасности – основные принципы"[13] рассказала о том, что такое культура кибербезопасности, и представила ряд возможных ролей различных заинтересованных сторон в информационном обществе в создании глобальной культуры кибербезопасности. Она выделила девять элементов создания культуры кибербезопасности, названных в Резолюции 57/239 (2002 г.) Генеральной Ассамблеи ООН "Создание глобальной культуры кибербезопасности" и Резолюции 58/199 (2004 г.) Генеральной Ассамблеи ООН "Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур". Эти девять элементов включают: a) осведомленность; b) ответственность; c) реагирование; d) этику; e) демократию; f) оценку риска; g) проектирование и внедрение средств обеспечения безопасности; h) управление обеспечением безопасности; и i) переоценку. В этих резолюциях государствам – членам ООН и соответствующим международным организациям предлагается принять меры для создания, развития и внедрения глобальной культуры кибербезопасности, сотрудничая между собой, и далее учитывать эти элементы при подготовке к двум этапам Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО)[14] в 2003 и 2005 годах. В итоговых документах двух этапов ВВУИО подчеркивается важность создания доверия и безопасности при использовании ИКТ и подтверждается решимость стран содействовать развитию культуры безопасности.

21 В своем докладе г-жа Сунд упоминала различные возможные роли для правительств в содействии развитию культуры кибербезопасности, в том числе: играть центральную роль в координации и реализации национальной стратегии кибербезопасности; обеспечивать гибкость и адаптируемость национальной политики; координировать обязанности органов власти и государственных департаментов; разрабатывать новое (или адаптировать имеющееся) законодательство для криминализации злоупотребления ИКТ; защищать права потребителей; обеспечивать защиту граждан страны; и руководить деятельностью по сотрудничеству в области кибербезопасности на национальном, региональном и международном уровнях. Что касается участия частного сектора в разработке национального подхода к обеспечению кибербезопасности, г-жа Сунд далее отметила, что, поскольку инфраструктуры ИКТ во многих странах находятся в собственности частного сектора и эксплуатируются им, участие этого сектора в создании национальной и глобальной культуры кибербезопасности играет решающую роль. Для эффективности мер по

---

13 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/sund-promoting-a-culture-of-cybersecurity-sofia-oct-08.pdf.

14 http://www.itu.int/wsis/.

обеспечению кибербезопасности требуется глубокое понимание всех аспектов сетей ИКТ, и поэтому специальные знания частного сектора и его участие имеют огромное значение для разработки и внедрения национальных стратегий кибербезопасности. Далее г-жа Сунд отметила, что правительства и деловые круги должны содействовать гражданам в получении информации относительно того, как защитить себя в онлайновом режиме. Хотя кибербезопасность по своей сути является совместной обязанностью, при наличии соответствующих инструментов каждый участник информационного общества отвечает за то, чтобы не терять бдительности и защищать себя.

22 Илари Патрик Линди, старший специалист по взаимоотношениям с отраслью и международными организациями (ENISA), рассказал о задаче ENISA по содействию развитию культуры информационной безопасности в Европе в своем докладе "Повышение осведомленности о создании культуры кибербезопасности: работа ENISA в последнее время"[15]. Г-н Линди сообщил о уже проделанной работе и о проводящихся инициативах в области повышения осведомленности по вопросам безопасности, с учетом того что повышение осведомленности всех заинтересованных сторон в государствах-членах является одной из основных целей ENISA для повышения потенциала органов ЕС и государств-членов в сфере безопасности. В этом отношении, продолжил г-н Линди, ENISA стремится стимулировать, ускорять, содействовать решению проблем кибербезопасности, выполнять функции советника и координатора. Повышение осведомленности и обеспечение понимания рисков и того, какие инструменты можно применять для защиты от угроз, является первой линией защиты безопасности информационных систем и сетей, сказал он.

23 Работа ENISA в области повышения осведомленности включает помощь в мониторинге прогресса на национальном уровне, предоставлении обзора образцов наилучшей практики, осуществляемых или планируемых государственными и частными организациями, разработке планов распространения этих образцов, а также обеспечении материала, который может быть адаптирован для содействия работе различных организаций и осуществлению инициатив по повышению осведомленности. ENISA также содействует внедрению культуры информационной безопасности в государствах-членах, призывая пользователей действовать ответственно и тем самым работать в условиях большей безопасности. Далее г-н Линди рассказал про инициативу создания Сообщества по повышению осведомленности. Сообщество по повышению осведомленности представляет собой сеть специалистов по информационной безопасности из государственных и частных организаций в 38 странах, которые обмениваются информацией по передовому опыту ЕС и инициативам по повышению осведомленности. Ее участники общаются, используя бюллетени, участвуя в ежемесячных селекторных совещаниях и принимая участие в мероприятиях, организуемых для Сообщества.

Джейнис Ричардсон, представитель организации European Schoolnet и координатор инициативы "Более безопасный интернет", представила доклад "Просвещение относительно онлайновой безопасности при подходе с участием многих заинтересованных сторон"[16]. Она рассказала о деятельности, проводимой в настоящее время в рамках Insafe, и подробнее остановилась на целях Insafe по повышению осведомленности в Европе и за ее пределами. Insafe представляет собой европейскую сеть центров по повышению осведомленности, созданную в 2004 году Европейской комиссией в рамках программы Европейской комиссии "Более безопасный интернет" для содействия безопасному, ответственному использованию онлайновых технологий, в особенности со стороны детей и молодежи. Г-жа Ричардсон представила применяемый Insafe для содействия развитию культуры кибербезопасности подход, который включает три основных элемента: 1) предоставление информации; 2) принятие мер и интеграцию в существующие виды практики; и 3) пропагандистскую деятельность. Последние четыре года сеть играет ведущую роль в мероприятиях по безопасности интернета в Европе и во всем мире, в том числе в рамках инициатив, проводимых в связи с Днем более безопасного интернета, который ежегодно отмечается в феврале более чем в 50 странах, отметила выступающая. Следующий День более безопасного интернета пройдет 10 февраля 2009 года.

---

15 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/lindy-enisa-awareness-sofia-oct-08.pdf.

16 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/richardson-insafe-sofia-oct-08.pdf.

25 Insafe также выполняет функции эксперта и наблюдателя при Отделе по средствам массовой информации информационному обществу Совета Европы и внес значительный вклад в создание многоязычного Справочника по интернет-грамотности, который был издан на восьми языках и распространялся по всему миру и послужил основой для недавно разработанной игры по онлайновой безопасности "Прогулка через Wild Web Woods"[17]. Также в 2008 году в сотрудничестве с оператором кабельных сетей Liberty Global Inc. Insafe разработал комплект материалов по электронной безопасности, в который входят рассказы и игры для детей 6–12 лет и руководство для родителей. Комплект материалов уже опубликован на 10 языках. Г-жа Ричардсон отметила, что в последнее время Insafe работает с консорциумом из 14 основных компаний, от Google до Vodafone, над созданием нового веб-сайта для учителей под названием TeachToday[18]. Этот сайт специально предназначен для удовлетворения разнообразных потребностей учителей, стремящихся обеспечить, чтобы их ученики получали максимально возможную пользу от технологий, но хорошо осознающих, какие опасности в них таятся для неосторожных.

26 Соланж Гернаути-Эли, профессор факультета бизнеса и экономики Лозаннского университета, Швейцария, представила доклад на тему "Культура кибербезопасности: от политики к практике"[19], в котором рассказывается о важности просвещения применительно к созданию культуры кибербезопасности и построению безопасного и открытого для всех информационного общества. Отсутствие ноу-хау и понимания всех аспектов кибербезопасности, т. е. технических, правовых, организационных и связанных с человеческим фактором аспектов, является серьезным недостатком инфраструктуры, расширяющим "цифровой разрыв", заявила она, подчеркнув далее, что развивающиеся и наименее развитые страны сталкиваются с серьезными проблемами, стремясь соответствовать требованиям мирового рынка без надлежащей кибербезопасности. Культура кибербезопасности должна стать неотъемлемой частью реагирования на киберугрозы на национальном и глобальном уровнях, касающиеся основных экономических, правовых и социальных вопросов в информационном обществе. В этом качестве она является важным компонентом, необходимым странам, готовящимся ответить на вызовы, которые связаны с развертыванием ИКТ, их использованием и злоупотреблением ими. В настоящее время, отметила г-жа Гернаути-Эли, основное внимание уделяется повышению осведомленности, что необходимо, но не достаточно. Для того чтобы инициативы по просвещению и повышению осведомленности были эффективными, они должны быть доступными и адресными для всех групп заинтересованных сторон. Следует предпринимать усилия и вкладывать средства для просвещения и профессиональной подготовки всех членов информационного общества, от лиц, принимающих решения и лиц, ответственных за разработку политики, политических лидеров, специалистов в области правосудия и сотрудников полиции, до граждан, конечных пользователей, детей и лиц пожилого возраста.

27 Чтобы решать национальные и международные проблемы кибербезопасности, на национальном уровне надо принимать конкретные меры с целью повышения потенциала различных субъектов, отметила выступающая. В настоящее время в развивающихся странах большинство конечных пользователей ИКТ не понимают проблем безопасности и не обладают навыками и инструментами для надлежащей защиты своих активов. У них нет средств для укрепления доверия к инфраструктурам и услугам ИКТ, и поэтому они вынуждены полагаться на продукты и механизмы, с которыми не умеют обращаться, и на решения, которые были им навязаны по коммерческим соображениям. Таким образом, заявила г-жа Гернаути-Эли, безопасность базируется на незаметности. Завершая свой доклад, она привела ряд основополагающих рекомендаций для эффективного содействия созданию культуры кибербезопасности. В их числе: необходимость далее просвещать конечных пользователей; повышать осведомленность общества в сфере безопасности для изменения онлайнового поведения конечных пользователей; снабжать конечных пользователей инструментами и материалами, необходимыми для ответственного онлайнового поведения; и в целом уделять основное внимание центрической модели безопасности конечного пользователя в данных технических и правовых условиях, с тем чтобы пользователь мог решить, что является разумным поведением, на основании собственных ресурсов.

---

17 http://www.wildwebwoods.org.

18 http://www.TeachToday.eu.

19 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/ghernaouti-helie-education-sofia-oct-08.pdf.

Заседание 3: Партнерство государственного и частного секторов

28 В настоящее время в условиях приватизации огромное большинство сетей ИКТ в каждой стране находятся во владении частного сектора и эксплуатируются им. Ключевым элементом национальной структуры кибербезопасности и CIIP является участие частного сектора и органов государственного управления в пользующихся доверием форумах для рассмотрения общих национальных задач по безопасности. Основой успешного партнерства государственного и частного секторов является доверие, которое необходимо для установления, развития и поддержания отношений совместного пользования между частным сектором и правительством. Заседание 3, где подробно рассматривались преимущества, а также проблемы, связанные с партнерством частного и государственного секторов, вел Красимир Симонски, заместитель председателя Государственного агентства информационных технологий и связи (ГАИТС), Болгария. Г-н Симонски отметил важность партнерства государственного и частного секторов для развития ИКТ и роль, которую оно способно сыграть в создании национального потенциала кибербезопасности.

29 Первый доклад на третьем заседании был сделан с применением удаленного доступа и онлайновых программных средств профессиональной подготовки Владимиром Радуновиком, DiploFoundation, Мальта. В своем докладе "Тематическое исследование по вопросам кибербезопасности и образования: развитие национального потенциала"[20] он обсудил ряд основных компонентов, которые следует рассматривать в отношении служащих целям развития образования и профессиональной подготовки в области кибербезопасности. В отношении проблем образования в этой области г-н Радуновик подчеркнул необходимость ввести межпрофессиональное общение в программу обучения кибербезопасности, в том числе в учебные курсы и в профессиональную подготовку, а также включать в состав групп учащихся и участников представителей различных заинтересованных сторон, предоставляя подготовку другим профессиональным и институциональным группам. Он также отметил необходимость расширения использования онлайновых инструментов для профессиональной подготовки по вопросам кибербезопасности и создания сообществ для культуры кибербезопасности. Г-н Радуновик также указал, что, основываясь на опыте профессиональной подготовки, которую DiploFoundation проводила по другим относящимся к интернету темам, когда коллективу предлагается проводить обучение собственными силами, причем опытный член коллектива выступает в качестве посредника между экспертами и начинающими подготовку участниками, участники обычно лучше воспринимают материал. Это, в сочетании с концепцией обучения на практике, когда профессиональная подготовка сочетается с практической деятельностью, успешно использовалось в других областях и может быть полезно применительно к кибербезопасности.

30 В своем докладе г-н Радуновик далее подчеркнул необходимость разработки национального потенциала кибербезопасности. В связи с этим он упомянул об использовании существующих инструментов и материалов, таких как Инструмент МСЭ по национальной самооценке в области кибербезопасности, о дальнейшем развитии учебных материалов на базе этой документации с соответствующими курсами, исследованиями в области политики и обучением методом погружения в качестве основы для практической последующей деятельности по инициативам и видам деятельности, проводимой в той или иной стране. В этом контексте он также представил обзор того, как могут выглядеть возможная программа профессиональной подготовки и связанные с ней курсы, а также привел дополнительные подробности относительно того, что могло бы войти в совместные онлайновые исследования по развитию национального потенциала кибербезопасности и как их можно было бы проводить.

31 Чери Макгуайр, главный специалист по вопросам стратегии в области кибербезопасности, Trustworthy Computing, Программа защиты особо важной инфраструктуры, Microsoft, в своем докладе представила обзор ряда "Тематических исследований партнерства государственного и частного секторов"[21]. Г-жа Макгуайр начала свой доклад с рассказа о Программе защиты особо важной инфраструктуры фирмы Microsoft, задачей которой является создание доверия и согласование действий органов государственного управления и поставщиков особо важной инфраструктуры. Обычно для партнерства государственного и частного секторов требуется, чтобы все стороны осознали ключевые аспекты терминов "государственный и частный секторы" и "партнерство", с тем

---

20 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/radunovic-diplofoundation-education-sofia-oct-08.pdf.

21 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/mcguire-case-studies-sofia-oct-08.pdf.

чтобы предоставить структуру, процессы и обстановку, необходимую для доверительного сотрудничества. Партнерство должно согласовать требования, приоритеты, цели и задачи отрасли и органов государственного управления, быть гибким и способным к адаптации для реагирования на меняющиеся риски, быть полезным как для органов государственного управления, так и для отрасли, а также уделять особое внимание постоянному совершенствованию и оценке извлекаемых уроков. После более общего рассмотрения основных требований, которые партнерство государственного и частного секторов должно выполнить, чтобы добиться успеха, г-жа Макгуайр привела примеры инициатив в области кибербезопасности и CIIP, в которых она участвовала на национальном и международном уровнях.

32 Она упомянула о таких партнерствах национального уровня, как Японский координационный центр групп быстрого реагирования на нарушения компьютерной защиты (JP-CERT) Японский национальный центр безопасности инфраструктуры, Австралийская консультативная группа по обеспечению инфраструктуры, Центр по защите национальной инфраструктуры и Информационная биржа по безопасности продавцов Соединенного Королевства, а также Консультативный совет по партнерству в области особо важной инфраструктуры, Сеть безопасности и Информационная биржа и Национальный консультативный комитет по безопасности электросвязи в Соединенных Штатах. Г-жа Макгуайр также рассказала о двух партнерствах частного сектора – ICASI и SafeCode. Промышленный консорциум по содействию безопасности интернета (ICASI)[22] был учрежден группой глобальных продавцов ИТ как пользующийся доверием форум для решения проблем безопасности международного уровня, относящихся к различным продуктам. Форум повышает способность продавцов ИТ решать сложные проблемы в сфере безопасности, чтобы лучше защищать предприятия, органы государственного управления, граждан и поддерживающие их особо важные инфраструктуры ИТ. Инициатива "Форум страхования программного обеспечения для совершенства кодов (SafeCode)[23] рассчитана на повышение доверия к продуктам и услугам ИКТ путем продвижения испытанных методов страхования программного обеспечения, выявляя передовой опыт разработки и поставки более безопасного и надежного программного обеспечения, аппаратного обеспечения и услуг и содействуя его распространению.

33 Виктор Минин, представитель Ассоциации по информационной безопасности, Российская Федерация, в своем докладе, озаглавленном "Роль НПО в сотрудничестве между правительственными органами и сектором кибербезопасности"[24], рассказал о некоторых направлениях деятельности, в которых участвует базирующаяся в России Ассоциация по информационной безопасности (АИБ). Организации, представленные в АИБ, могут в соответствии с лицензией выданной Федеральным агентством правительственной связи и информации и Государственной технической комиссией, предоставлять услуги в области информационной безопасности, в частности охранять секретную и конфиденциальную информацию, осуществлять исследовательские и другие проекты в области информационной безопасности, реализовывать проекты, предусматривающие использование данных, которые составляют государственную тайну; изучать, разрабатывать и продвигать на рынке криптографические продукты, а также предоставлять послепродажную техническую поддержку.

34 В своем докладе г-н Минин подчеркнул важность просветительской деятельности применительно к информационной безопасности и отметил, что АИБ также проводит ряд инициатив по повышению осведомленности. Он подчеркнул необходимость ответственного онлайнового поведения, заявив, что "если не чистить зубы каждый день, разовьется кариес. Аналогичным образом, если вы ежедневно пользуетесь ИКТ, надо уделять внимание ряду базовых моментов". Кроме того, когда люди ездят в другие страны, им для идентификации выдаются паспорта, но когда пользователи ИКТ входят в киберпространство, они делают это анонимно, и пользователи интернета должны лучше понимать опасности, которым они при этом подвергаются. Затем выступающий задался вопросом: кто в интернете плохие парни и плохие девчонки? В этом отношении АИБ не только разрабатывает инструменты для выслеживания киберпреступников, но и разрабатывает профили преступников, которые могут привести к принятию профилактических мер и смягчению последствий этих преступлений.

---

22 http://www.icasi.org.

23 http://www.safecode.org.

24 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/minin-ngo-cooperation-sofia-oct-08.pdf.

35 Джоди Уэстби, генеральный директор компании Global Cyber Risk, Соединенные Штаты Америки, в своем докладе "Культура партнерств государственного и частного секторов"[25] заявила, что в партнерствах государственного и частного секторов могут и должны участвовать все киберпользователи, от граждан до корпораций, правоохранительных органов и поставщиков особо важных инфраструктур. Выступающая отметила, что компьютеры могут применяться в преступной деятельности в киберпространстве тремя основными способами: 1) как объект правонарушения, когда нарушаются конфиденциальность, целостность и доступность данных, приложений и сетей; 2) как инструмент совершения преступления, в целях мошенничества, детской порнографии, заговора и т. п.; и 3) имея к преступлению косвенное отношение, но представляя существенную важность для охраны правопорядка, особенно в отношении доказательств. Реалии киберпространства ясно показывают, что все должны работать вместе, добавила она. В этом отношении партнерство государственного и частного секторов должно быть частью культуры кибербезопасности и неотъемлемой частью любой программы безопасности и плана реагирования на инциденты. Деятельность в области кибербезопасности и реагирование на киберугрозы, продолжила она, требуют больше ресурсов, чем имеется у отдельно взятой единицы. В целом партнерства государственного и частного секторов должны быть более открытыми для участия, чем сегодня, сказала она. Сотрудничество между государственным и частным секторами также важно для обеспечения кибербезопасности в глобальном масштабе. "Ни одна атака – не остров", продолжила г-жа Уэстби, подчеркивая тот факт, что каждый инцидент действительно представляет собой проблему глобального масштаба, для решения которой требуются партнерства государственного и частного секторов, что в свою очередь предусматривает трансграничное сотрудничество.

36 Г-жа Уэстби также обратила внимание участников на ряд моделей партнерства государственного и частного секторов, которые применялись в других секторах экономики, в особенности при приватизации государственных предприятий. Она выделила некоторые достоинства и недостатки этих моделей, которые интересно было бы рассмотреть также применительно к партнерствам государственного и частного секторов в области кибербезопасности. Устойчивость партнерств государственного и частного секторов является реальной проблемой, добавила выступающая, отметив полезность центров совместного использования информации и обмена информацией и указав на некоторые из проблем, с которыми сталкиваются эти центры. Общая цель этих центров, для достижения которой они были изначально созданы, заключается в сборе и анализа информации об угрозах, уязвимых местах, инцидентах, контрмерах и передовом опыте в области информационной безопасности, а также в совместном использовании этих данных с членами. Она отметила, что может казаться необходимым пересмотреть структуру и стимулы, благодаря которым различные участники обмениваются информацией в этих центрах, чтобы не допустить нарушения своей устойчивости. Поскольку многие отрасли все в большей степени зависят друг от друга, от электричества и электросвязи и т. п., возрастает потребность изучить вопрос о том, как заинтересованные стороны могут добиться более согласованного подхода к обеспечению кибербезопасности, заключила она.

37 Вечером первого полного дня работы форума участники были приглашены Председателем Государственного агентства информационных технологий и связи на прием в Центральный военный клуб.

Заседание 4: Правовая основа и обеспечение соблюдения действующего законодательства

38 Надлежащее национальное законодательство, международная координация в области права и обеспечение соблюдения действующего законодательства – все это важные элементы, касающиеся предотвращения, обнаружения и реагирования на киберпреступления и злоупотребления ИКТ. В связи с этим требуется обновление уголовного законодательства, процедур и правил для урегулирования инцидентов в области кибербезопасности и реагирования на киберпреступления. В результате во многих странах в уголовные кодексы были внесены изменения или идет процесс принятия изменений в соответствии с международными конвенциями и рекомендациями. На заседании 4 подробно рассматривалась необходимость прочной правовой основы и эффективного обеспечения соблюдения действующего законодательства, а также анализировались некоторые подходы к правовой основе, применяемые на национальном уровне, и изучались потенциальные

---

25 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/westby-culture-public-private-sofia-oct-08.pdf.

области, на которые могут быть направлены усилия по международной координации в области права. Заседание вел Эхаб Элсонбати, старший судья Даманхурского суда, Египет, который представил выступавших на заседании и подчеркнул необходимость обновления действующих законов и, по мере надобности, разработки нового законодательства для решения обостряющихся проблем, связанных со злоупотреблением ИКТ.

39 Хенрик Касперсен, профессор Амстердамского университета, Нидерланды, член и бывший председатель Комитет по Конвенции о киберпреступности, выступил на заседании с первым докладом – обзором "Конвенции о киберпреступности Совета Европы"[26]. Он отметил, что изначально, когда была начата работа над текстом Конвенции, цель заключалась в создании глобальной конвенции. На настоящее время 47 стран подписали и 23 ратифицировали Конвенцию, и этого, заявил выступающий, достаточно на данный момент для дальнейшего продвижения документа. Среди подписавших Конвенцию – государства – члены Европейского союза и страны Группы семи. Он также отметил, что страны, не входящие в Европейский союз, используют Конвенцию в качестве модели при пересмотре и обновлении своего законодательства и разработке нового законодательства. Конвенция о киберпреступности направлена на: a) согласование материального уголовного права для обеспечения отсутствия мест укрытия данных и рассмотрения обоюдного признания деяния преступлением и кибербезопасности в узком и широком смысле слова; b) согласование деятельности подразделений, занимающихся расследованиями, с тем чтобы обеспечить потенциал для сбора доказательств в электронной форме, их сохранности, производства данных, в том числе данных по трафику, надзора в интернете и т. п.; и c) международное сотрудничество на базе Конвенции с существующими двусторонними и многосторонними документами и экстренная помощь силами Сети круглосуточной помощи при преступлениях в области высоких технологий и другими способами.

40 Г-н Касперсен упомянул, что Конвенция о киберпреступности считается одной из наиболее эффективно действующих конвенций в портфеле Совета Европы. Затем он задался вопросом: совершенна ли Конвенция, и отметил, что имеются проблемные области, к которым относятся экстерриториальная юрисдикция (применительно к статье 22 Конвенции), юрисдикция в отношении исполнения (применительно к статье 32 Конвенции) и возможное отсутствие срочности при относительно низком показателе раскрытых преступлений, на которые можно было бы ссылаться, а также акцент на внутригосударственные дела. Г-н Касперсен также рассказал о проекте Совета Европы по борьбе с киберпреступностью. Проект по борьбе с киберпреступностью охватывает ряд направлений деятельности по координации борьбы с киберпреступностью, в том числе: консультации с отраслью в отношении возможных кодексов практики; сотрудничество с правоохранительными органами; обмен опытом, сведениями о методах и инструментах; предоставление профессиональной подготовки и правовых консультаций; и создание новых форумов, таких как Комитет Конвенции по киберпреступности, где обсуждаются связанные с киберпреступностью вопросы.

41 Марко Герке, лектор Кельнского университета, Германия, представил доклад на тему "Правовая основа и основные принципы обеспечения соблюдения действующего законодательства", в котором уделил основное внимание тому, что в настоящее время происходит в международном сообществе, в особенности в отношении усилий, предпринимаемых странами для пересмотра действующих законов и разработки нового законодательства для криминализации злоупотребления ИКТ. Г-н Герке отметил, что постоянно появляются новые правонарушения и новые проблемы, когда дело касается интернета, и поэтому необходимо постоянно пересматривать и обновлять национальное законодательство. Страны и заинтересованные стороны, которых это касается, должны в первую очередь изучить применяемые технологии и понять, как ими злоупотребляют, а затем защитить пользователей с помощью нового законодательства, не забывая, что между признанием деяния преступлением и изменением законодательства всегда проходит некоторое время. Хотя многие связанные с интернетом проблемы требуют правовых решений, продолжил он, не все проблемы требуют правовых решений. Ввиду этого страны не должны считать преступлением то, что не считается преступлением за пределами интернета. Г-н Герке отметил, что правовая основа создает рамки для расследования, судебного преследования и сдерживания киберпреступности, содействия кибербезопасности и поощрения торговли.

---

26 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/kaspersen-cybercrime-convention-sofia-oct-08.pdf.

42 Говоря о национальном, региональном и международном законодательстве по киберпреступности, г-н Герке подчеркнул важность и необходимость дальнейшего согласования законодательства. Он отметил, что существует ряд международных инициатив по кибербезопасности и борьбе с киберпреступностью и что все эти различные инициативы должны сыграть свою роль. В отношении Конвенции о киберпреступности, ранее обсуждавшейся г-ном Касперсеном, г-н Герке заметил, что она охватывает основные области законодательства по киберпреступности (материальное уголовное право, процессуальное право и международное сотрудничество) и может применяться к странам обычного права и гражданского права. Г-н Герке далее отметил, что для развивающихся стран серьезной задачей является нахождение адекватных вариантов реагирования на угрозу киберпреступности. Разработка и реализация национальной стратегии кибербезопасности, включая борьбу с киберпреступностью, требует времени и может обойтись довольно дорого, что в свою очередь может помешать странам принять необходимые меры. Поэтому возрастает важность того, чтобы все страны разрабатывали потенциал и компетенцию, необходимые для пересмотра законодательства, расследования случаев незаконного использования сетей или злоупотребления ими и обеспечения наказания преступников, которые совершают атаки на сети или эксплуатируют их.

43 Мэтью Ламберти, координатор для Восточной Европы по обеспечению соблюдения действующего законодательства в области интеллектуальной собственности, Департамент юстиции США, посольство Соединенных Штатов Америки в Болгарии, далее представил доклад на тему "Правовая основа и обеспечение соблюдения действующего законодательства: страновые тематические исследования"[27], в котором рассказал о некоторых уроках, извлеченных из работы, проводимой им в 20 странах Центральной и Восточной Европы. Г-н Ламберти отметил, что в странах этого региона обычно имеются законы, охватывающие киберпреступность, и что во многих странах выделены агенты для борьбы со специализированными компьютерными преступлениями, но в большинстве стран нет сил для обеспечения соблюдения действующего законодательства. Если не обеспечить соблюдение законов в этой важной сфере, можно потерять бизнес и инвестиции. Далее он отметил, что многие связанные с кибербезопасностью и киберпреступностью дела носят трансграничный характер, и поэтому расследования должны иметь глобальный охват.

44 Г-н Ламберти подчеркнул важность пересмотра и обновления законов для охвата новых и возникающих технологий. Он отметил, что Конвенция Совета Европы о киберпреступности является важным инструментом и что население стран региона знает о существовании Конвенции, но эти страны не обязательно непосредственно применяют ее для направления своей работы по криминализации злоупотребления ИКТ. Г-н Ламберти привел ряд примеров трансграничного сотрудничества в расследованиях и упомянул о расследовании, в котором участвовали сотрудники правоохранительных органов из Соединенных Штатов и Румынии, отметив, что такое сотрудничество было возможно только под эгидой Конвенции о киберпреступности и Сети круглосуточной помощи при преступлениях в области высоких технологий. В связи с этим он также поделился соображениями о некоторых случаях расследования и судебного преследования, в которых он участвовал вместе с представителями отрасли, и рассказал о том, как этот подход способен различными способами сэкономить деньги для правительств стран.

45 Явор Колев, главный инспектор, Руководитель подразделения по киберпреступности, Национальная полицейская служба, Болгария, в своем докладе, озаглавленном "Органы Болгарии, обеспечивающие соблюдение действующего законодательства по противодействию киберпреступности: Структура и правовые основы"[28], поделился информацией о структуре, законодательстве и обеспечении соблюдения действующего законодательства, которые Болгария ввела в действие для борьбы с растущим числом преступлений, связанных с киберпространством. Он отметил, что хотя для Болгарии это совершенно новая сфера деятельности, уже 50 человек работают в этой сфере, и в ближайшие месяцы к работе в этой области будут привлекаться новые люди. Г-н Колев сообщил, что в каждой дирекции, относящейся к Министерству внутренних дел, работает по меньшей мере один человек, прошедший специальную подготовку для работы по борьбе с киберпреступностью.

---

27 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/lamberti-united-states-case-study-sofia-oct-08.pdf.

28 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/kolev-bulgaria-enforcement-sofia-oct-08.pdf.

46 Г-н Колев также упомянул о том, что существующая Сеть круглосуточной помощи при преступлениях в области высоких технологий является очень полезным инструментом и ресурсом в повседневной работе, и привел ряд примеров того, как Болгария использует эту сеть для проведения расследований. Он отметил, что помощь, получаемая в рамках Сети, является эффективным способом обеспечения того, что данные сохраняются верно и оперативно для поддержки ведущихся расследований. Относительно пользователей услугами Сети г-н Колев упомянул, что группа по борьбе с киберпреступностью, которую он возглавляет, получает много запросов на расследование связанных с компьютерами преступлений. Основным юридическим документом, на который ведущие расследования полагаются при расследовании и выявлении этих преступлений, является болгарский уголовный кодекс. Некоторые статьи его в большей степени актуальны, отметил он, приведя пример статьи 159 о порнографии, в первую очередь формулировки, относящейся к детской порнографии, а также к наказаниям за эти и связанные с ними преступления.

47 Эхаб Элсонбати, старший судья Даманхурского суда, Египет, в своем докладе "Обзор правовых проблем"[29] рассказал о некоторых правовых инструментах, применяемых в настоящее время для борьбы с киберпреступностью в Египте. Он отметил, что, поскольку масштабы киберпреступности растут быстрее, чем обычной преступности, а особо важные инфраструктуры все чаще работают на компьютерах и сетях и управляются ими, относящиеся к киберпреступности нормы египетской правовой системы в настоящее время пересматриваются. Все страны, заявил выступающий, должны обеспечить, чтобы их уголовное право было пересмотрено для учета особого характера киберпреступности. Пересмотр и обновление можно провести, изменяя некоторые статьи, относящиеся к классическим преступлениям, применительно к новым средствам, упраздняя некоторые другие, уже не соответствующие, и создавая новые нормы для полностью новых вопросов.

48 Г-н Элсонбати также отметил, что следует пересмотреть уровни наказания, как тюремного заключения, так и штрафов. Далее он подчеркнул значение разработки программ профессиональной подготовки для служащих правоохранительных органов, прокуратур, а также для судей и законодателей. Международный характер киберпреступности, продолжил он, вызывает потребность в решении международного уровня, которое охватывало бы нормы существа, процедуры и международного сотрудничества. В связи с этим он упомянул работу, проводимую в Египте, и заявил, что с нетерпением ожидает появления современного египетского закона о киберпреступности.
В заключение г-н Элсонбати упомянул Сеть круглосуточной помощи при преступлениях в области высоких технологий как полезную контактную сеть для работы с делами, которые предполагают трансграничный сбор электронных доказательств.

Заседание 5: Организационная структура и возможности устранения инцидентов

49 Ключевая деятельность в области кибербезопасности на национальном уровне требует обеспечения готовности к киберинцидентам, их обнаружения и устранения, а также реагирования на них путем создания возможностей для наблюдения, предупреждения инцидентов и реагирования на них. Эффективное устранение инцидентов требует учета аспектов, касающихся финансирования, наличия людских ресурсов, профессиональной подготовки, технического потенциала, взаимоотношений между органами государственного управления и частным сектором, а также правовых требований. Необходимо сотрудничество на всех уровнях государственного управления, а также сотрудничество с частным сектором, научным сообществом, региональными и международными организациями в целях повышения осведомленности о возможных атаках и способах борьбы с ними. На заседании 5, проходившем под председательством Ярослава Пондера, координатора для Европы, Сектор развития электросвязи МСЭ (МСЭ-D), был рассмотрен передовой опыт, организационные структуры и соответствующие стандарты, а также технические, управленческие и финансовые аспекты создания на национальном, региональном и международном уровнях потенциала для наблюдения, предупреждения инцидентов и реагирования на них.

---

29 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/elsonbaty-legal-challenges-sofia-oct-08.pdf.

50 Генеральный секретарь Ассоциации сетей Центральной и Восточной Европы (CEENet) и представитель Постоянной группы заинтересованных сторон ENISA, Яцек Гаевски, Польша, открыл заседание презентацией "Руководства ENISA по поэтапному созданию национальных CERT/CSIRT"[30]. Выпущенное в 2006 году, Руководство по поэтапному созданию групп реагирования на инциденты в сфере компьютерной безопасности (CSIRT)/групп реагирования на компьютерные инциденты (CERT) имеет целью охватить все аспекты услуг, предоставляемых CERT, а также необходимые этапы от управления предприятием, управления процессами до технических аспектов создания CERT. Руководство включает тематические исследования, упражнения, а также практический план реализации всего проекта. CERT являются важнейшим структурным элементом защиты сетевых и информационных систем, отметил г-н Гаевски. Требуется более широкое географическое распределение CERT при более активном внедрении в самые различные сектора общества, а именно: в научные круги, органы государственного управления, а также сферу бизнеса, – сказал он. CEENet является объединением национальных организаций, занимающихся в основном организацией академических, научно-исследовательских и образовательных сетей и в настоящее время включающей 23 национальные научно-исследовательские и образовательные сети в странах Центральной и Восточной Европы. Поэтому CEENet является как раз тем органом, который может оказать поддержку в создании CERT/CSIRT в данном регионе. В 2007 году CEENet приступила к реализации проекта в поддержку создания новых CERT для академической сети в этих странах. В результате, в CEENet настоящее время ведет три проекта в данном регионе и планирует начать четвертый проект для стран Магриба.

51 На сегодняшний день в каждой стране CEENet подготовлено от 1 до 3 сотрудников на основе учебного материала, содержащегося в Руководстве ENISA, а также преходящего материала, распространенного ассоциацией TERENA. Г-н Гаевски отметил, что когда CEENet вместе с соответствующими странами занималась созданием академических CERT, то последние часто служили в качестве первого шага в создании национальных CERT. Г-н Гаевски завершил свое представление кратким обзором создания CERT в некоторых странах СНГ. Он отметил, что, хотя одни CERT функционировали весьма успешно, другие оказались не столь удачными и функционировали не достаточно устойчиво. Он отметил также, что от принятия решения о создании новой CERT до начала ее функционирования требуется приблизительно двухгодичный период. Кроме того, должен существовать вышестоящий орган, готовый помочь контролировать и поддерживать деятельность этой новой организации. Он сказал также, что существует не мало стран, в которых CERT/CSIRT отсутствуют, и призвал страны региона расширить эту сеть и создать свои собственные CERT.

52 Александр Золотников, руководитель подразделения информационной безопасности компании ТрансТелеКом, Российская Федерация, сделал представление на тему: "Противодействие киберпреступности: практические действия оператора магистральной сети связи"[31]. В своем представлении он затронул вопросы, касающиеся киберпреступности в глобальных информационных сетях, противодействия нежелательному онлайновому контенту и роли оператора связи в этом отношении. Г-н Золотников отметил, что информация, которую сегодня можно найти в интернете, в силу своей объективности, полноты, надежности, достоверности и благопристойности, фундаментальным образом влияет на развитие личности, а также на его или ее активную жизненную позицию. Вместе с тем появление нежелательного контента может оказать весьма негативное влияние на развитие людей и общества и в конечном итоге представлять угрозу для национальной безопасности страны. Такое положение вещей, сказал г-н Золотников, требует принятия активных и своевременных мер по борьбе с такими угрозами, исходящим из интернета. Далее г-н Золотников рассмотрел меры, которые могут быть приняты операторами электросвязи, в целях противодействия проблемам, связанным с этими угрозами, и обратил внимание на необходимость безотлагательной разработки средств борьбы с нежелательным контентом в интернете, особенно в тех случаях, когда речь идет о распространении детской порнографии.

---

30 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/gajewski-enisa-cert-toolkit-sofia-oct-08.pdf.

31 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/zolotnikov-content-sofia-oct-08.pdf.

53 Касаясь вопроса борьбы с распространением детской порнографии в Российской Федерации, он привел ряд статистических данных. Г-н Золотников дал оценку некоторых способов противодействия данной проблеме и предложил механизм, который, с точки зрения операторов электросвязи, может рассматриваться в качестве наиболее эффективного средства борьбы с нежелательным контентом, включающий необходимость принятия мер на уровне компании электросвязи, что обеспечивает максимальную компетентность и гибкость при разработке услуг.

54 Мауро Виньяти, аналитик MELANI, Федеральное бюро полиции Швейцарии, в своем представлении "Партнерские отношения между государственным и частным секторами: исследование на примере Швейцарии"[32] рассмотрел причины настоятельной необходимости обеспечения защиты важнейшей информационной инфраструктуры страны, а также меры, предпринимаемые Швейцарией для решения нарастающих проблем, связанных с CIIP. Он начал свое представление с рассмотрения различий между CIIP и CIP и тесной связи между ними и представил MELANI, являющейся центром оповещения и анализа состояния информационной безопасности в Швейцарии. MELANI функционирует с октября 2004 года и составляет ядро системы раннего оповещения Швейцарии, поскольку является неотъемлемой частью четырех основных составляющих политики в области информационной безопасности Швейцарии (т. е. предотвращение, ранее оповещение, управление в кризисных ситуациях и решение технических проблем). С начала 2008 года MELANI управляет также правительственной CERT, GovCERT.ch, которая служит в качестве центра технических знаний, отвечающего за устранение соответствующих технических инцидентов.

55 Г-н Виньяти отметил возрастание угроз системам централизованного контроля и сбора информации (SCADA) стран, подчеркнув при этом тот факт, что эти системы могут быть подвержены различного рода дистанционным манипуляциям и контролю с возможностью совершения атак, которые могут иметь самые серьезные последствия для общества. В этом отношении он поделился с участниками мнениями по поводу возможных проверок готовности, проведенных с использованием компьютерных систем. Касаясь вопроса о дискуссиях и видах деятельности, связанных с национальной информационной инфраструктурой, г-н Виньяти подчеркнул важность участия в этих дискуссиях всех заинтересованных сторон отрасли. В качестве примера он упомянул важное значение, которое придается в Швейцарии участию представителей финансового и банковского секторов в обсуждении вопросов CIIP.

Заседание 6: Национальная стратегия в области кибербезопасности

56 Электронные сети все чаще используются в преступных целях или для решения таких задач, которые могут нарушить целостность критической инфраструктуры и создать препятствия для широкого использования преимуществ ИКТ. Чтобы устранить эти угрозы и защитить инфраструктуры, каждой стране необходимо иметь всеобъемлющий план действий, который охватывал бы технические, правовые и политические вопросы, наряду с установлением регионального и международного сотрудничества. Какие вопросы должны быть учтены в национальной стратегии в области кибербезопасности и защиты особо важной инфраструктуры? Кто должен в этом участвовать? Имеются ли примеры основных принципов и подходов, которые можно было бы использовать? На заседании 6, проходившем под председательством Румена Трифонова, секретаря Координационного совета по вопросам информационного общества при Совете министров Болгарии, была предпринята попытка более детально изучить различные подходы, примеры передового опыта и основные элементы, которые могли бы помочь странам в разработке национальных стратегий в области кибербезопасности и защиты особо важной инфраструктуры. Основываясь на представлениях, сделанных во время предыдущих заседаний, участники 6-го заседания обсудили заключительный элемент организации национальных усилий в области кибербезопасности/CIIP, который объединяет другие компоненты, а именно: общую разработку национальной стратегии в области кибербезопасности.

---

[32] Слайды отсутствуют.

57 Первое представление на данном заседании было сделано Александром Доносом, директором государственного предприятия Центра специальной связи Молдовы, представившим "Исследование на примере Молдовы – Национальная стратегия в области информационной безопасности"[33]. В своем представлении он отметил некоторые риски для информационной безопасности и угрозы для информационного общества в целом, а именно: несанкционированный доступ к системе и ресурсам государственной информации; несанкционированная замена и удаление информации государственной важности; блокирование правительственных веб-сайтов и информационных систем, а также атаки хакеров, компьютерные вирусы и спам. Меры, принятые в Молдове для устранения этих угроз, включают внедрение цифровых подписей и создание необходимых условий для их использования, разработку защищенной системы электросвязи для государственных органов власти в городе Чисинау, а также создание основного центра правительственной информации в целях защиты важнейших государственных баз данных и информации.

58 В числе приоритетных мер по обеспечению безопасности в стране г-н Донос выделил необходимость дальнейшего продвижения в создании внутриведомственных систем информации, развитии систем связи государственных органов власти в стране и интегрирования информационной системы как центральных, так и местных органов власти. Он отметил также необходимость создания шлюзов безопасности для правительственного портала, а также создание национального центра для обеспечения информационной безопасности и связанного с ней управления системой связи государственных органов власти. Целью данного ситуационного центра, который будет размещаться в помещениях центра специальной связи государственного предприятия, сказал г-н Донос, является предотвращение и обнаружение проникновений в компьютеры и хакерских атак, разработка систем защиты от вирусов и спама, а также осуществление общего контроля и наблюдения за состоянием информационной безопасности на национальном уровне. Вся эта деятельность осуществляется в рамках инициативы, реализуемой под руководством президента страны и направленной на дальнейшее развитие системы электронного управления в государстве. Данный запланированный проект осуществляется в три этапа: 1) разработка инфраструктуры электронного правительства, которая уже завершена; 2) внедрение услуг электронного правительства, которое осуществляется в настоящее время, в частности, путем развертывания электронных услуг для граждан; и 3) дальнейшее развитие услуг электронного правительства. Для успешной реализации этих инициатив, направленных на обеспечение безопасной онлайновой среды в Молдове, необходимо сотрудничать с соседями, подчеркнул г-н Донос.

59 Валерий Конявский, директор Всероссийского научно-исследовательского института проблем вычислительной техники и информатизации (ВНИИПВТИ) Российской Федерации, рассмотрел некоторые "Новые подходы к обеспечению кибербезопасности"[34]. ПВТИ – это сеть научно-исследовательских организаций при Министерстве связи и массовых коммуникаций, занимающихся проведением научных исследований, решением проблем законотворчества в области электросвязи, проблем информационной безопасности, сертификации, компьютерных систем и сетей и т. д. Институт участвовал в разработке и реализации крупномасштабных национальных проектов, например, по созданию государственной сети компьютерных центров, в частности, центров коллективного пользования. Г-н Конявский отметил, что существует слишком много статистических данных по всем аспектам информационно-коммуникационных технологий, и зависимость от этих данных приводит к тому, что различные заинтересованные стороны выбирают неправильные меры реагирования. В тех случаях, когда реакция на существующие и возникающие угрозы является неадекватной, "клубника будет украдена, какой бы высокой ни была изгородь", – сказал он. К тому же, если заинтересованные стороны не знают точно, что находится под защитой, то соответствующие защитные меры и меры по реагированию вероятнее всего будут оставаться ошибочными. Поэтому, г-н Конявский призвал участников собрания внести осмысленные изменения в подходы, которые они используют в настоящее время, и впредь рассматривать компьютерный мир, не как природное явление, а как нечто рукотворное.

---

33 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/donos-moldova-case-study-sofia-oct-08.pdf.

34 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/konyavsky-new-approaches-sofia-oct-08.pdf.

60 Славчо Манолов, советник Председателя SAITC, Болгария, и кандидат в члены Правления ENISA в своем представлении рассмотрел "Политику болгарского правительства в области сетевой и информационной безопасности"[35]. Закон об электронном управлении, принятый в июне 2007 года, регулирует требования, касающиеся обеспечения сетевой и информационной безопасности в системах общедоступной информации в стране, и возложил на SAITC, как государственный орган, ответственность за эту область. Касаясь вопроса об общей деятельности в Болгарии по построению сетевого и информационного общества, г-н Манолов отметил, что принятая стратегия содержит отчетливые меры по обеспечению информационной безопасности, которые могут быть реализованы на двух уровнях: меры, относящиеся к центральному уровню реагирования, и меры на уровне административных органов. Меры на центральном уровне включают: a) создание централизованного органа управления национальной сетью электронной связи (NESM); b) создание национальной группы реагирования на инциденты в сфере компьютерной безопасности; создание единых условий для безопасного обмена электронными документами (ESOD); реализация национальной модели электронного управления данными для государственного управления посредством централизованно управляемых регистров; разработка единой политики в отношении центов послеаварийного восстановления работоспособности; создание центрального подразделения по контролю за сетевой и информационной безопасностью под эгидой SAITC и т. д. Уровень административных органов, в свою очередь, основывается на следующих принципах: a) внутренних правилах и руководящих указаниях в соответствии с системами спецификаций управления информационной безопасностью, предусмотренных стандартом ISO 27001:2005; b) специальной сертификации административных информационных систем и сетей Председателем SAITC и т. д.

61 Г-н Манолов рассказал также о создании болгарским правительством CSIRT, требовании регламента о создании CSIRT и о том, как правительство создавало основы для этой структуры при поддержке венгерской CERT и ENISA. Он отметил, что CSIRT будет также выполнять функции национальной CERT. Подход и политика болгарского правительства в области сетевой и информационной безопасности на уровне муниципальных образований и самого правительства в большей степени децентрализованы по сравнению с подходом Молдавии, представленным ранее, отметил г-н Манолов. Закон об электронном управлении и шесть связанных с ним нормативно-правовых актов создают прочную и функционально завершенную основу для соблюдения требований сетевой и информационной безопасности административных информационных систем. Эти требования направлены, главным образом, на обеспечение устойчивого обмена внутренними электронными административными услугами между администрациями, сказал г-н Манолов.

Заседание 7: Анализ и дискуссия: организация усилий в области национальной кибербезопасности/CIIP

62 Цель заседания 7 заключалась в том, чтобы рассмотреть и более подробно обсудить различные элементы, необходимые для разработки и организации национальных усилий в области кибербезопасности/CIIP, а также соответствующий инструментарий МСЭ для самостоятельной оценки положения в области национальной кибербезопасности /CIIP, выделив при этом основные моменты в представлениях, которые были сделаны в ходе различных заседаний и в исследованиях на примерах, посвященных отдельным странам, при подготовки к заключительным дискуссиям на данном собрании. Эти дискуссии были включены в заключительные дискуссии, состоявшиеся во время 10-го заседания, посвященного региональному и международному сотрудничеству, и 11-го заседания, посвященного подведению итогов собрания и определению некоторых конкретных шагов по дальнейшим действиям в области кибербезопасности в Европе и Содружестве независимых государств.

Заседание 8: Криминалистика и кибербезопасность

63 На заседании 8 был сделан обзор работы, проделанной в регионе в области криминалистики, касающейся кибербезопасности, анализа инцидентов и передового опыта по обеспечению соблюдения действующего законодательства. Ведущий заседания, Андреа Джирардини, консультант и эксперт в области компьютерной криминалистики Межрегионального научно-исследовательского института Организации Объединенных Наций по вопросам преступности и правосудия (UNICRI), открыл заседание, отметив, что киберкриминалистика является новой областью и что она ей останется.

---

35 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/manolov-bulgaria-strategy-sofia-oct-08.pdf.

64 Евгении Николов, доктор математических наук, директор национальной лаборатории по исследованию компьютерных вирусов Болгарии, в своем представлении, озаглавленном "Современные тенденции в атаках на важнейшую информационную инфраструктуру"[36] рассмотрел некоторые определения, используемые в области кибербезопасности и киберкриминалистики. Он представил также анализ некоторых инструментов, используемых для совершения атак, а также изменений, произошедших в этой области за последние несколько лет. Г-н Николов коснулся вопроса о масштабах этих атак в глобальных сетях, а также о том, как происходило преобразование вирусов и компьютерных червей в то, чем они в настоящее время являются. Он завершил свое представление описанием некоторых тенденций в области безопасности, а также набора инструментов и методов защиты информации, хорошо зарекомендовавших себя при защите от атак на информационную инфраструктуру. Он отметил необходимость применения упреждающего программного обеспечения для надежной защиты законных пользователей, рассказал о том, как блокировать атаки на сеть с ведущей машиной и устранить уязвимости системы безопасности, и перечислил некоторые инструменты, используемые для решения вопросов безопасности и достижения максимальной эффективности.

65 Алес Заврсник, научный сотрудник Института криминологии, факультет права, Словения, принял вместе с участниками собрания участие в обсуждении темы "Вмешательство системы уголовного правосудия перед лицом угроз кибербезопасности: панацея или ящик Пандоры?"[37]. В своем представлении он отметил, что в настоящее время общества используют целый ряд методов противостояния угрозам кибербезопасности, включающих повышение осведомленности общественности в вопросах кибербезопасности, создание безопасных технологий путем повышения безопасности протоколов, защиту сетей самыми различными способами и т. д. Однако лишь одних технических мер нерепрессивного характера, используемых частным сектором и технически грамотными людьми, не достаточно для обеспечения необходимого уровня информационной и сетевой безопасности, сказал он. Поэтому борьба с киберугрозами должна пользоваться поддержкой со стороны центральной системы по борьбе с преступностью и исполняться ею, т. е. системой уголовного правосудия, отметил он. Эта система является лишь одним звеном в цепи кибербезопасности, которое может помочь повысить кибербезопасность, однако наряду с этим такой ответ может вызвать нежелательные последствия, например, в виде нарушения гражданских свобод, повлиять на свободное использование интернета и создать проблемы с охраной общественного порядка.

66 В своем представлении г-н Заврсник хотел показать, почему киберкриминалистика должна занять свое место структуре системы уголовного правосудия, а также обратить внимание на некоторые проблемы, с которыми в настоящее время сталкивается профессия киберкриминалистики, ввиду неясностей, продолжающих сохраняться в этой области. В отношении электронного следа он попросил принять решения и договориться о том, как собирать скрытые и транзитные данные, как анализировать и осмысливать эту информацию и как ее защищать? Кроме того, он попросил разъяснить, как выявить подозреваемых, начиная от получения данных до виртуальной идентификации реального лица. Он довел также до сведения участников вопрос о том, как получить данные и информацию, переданные или хранящиеся в источнике. Попросив участников творчески подумать над вопросом о том, что представляет большую угрозу: растущая проблема киберпреступности или фактическая реакция на проблему кибербезопасности при принятии мер системой правосудия, он рассмотрел некоторые весьма реальные проблемы в этом отношении. В условиях отмены регулирования вопросов, касающихся специальных знаний, кто может проводить киберкриминалистический анализ, кто может предоставить руководящие указания по обработке цифровых доказательств, кто должен обеспечивать подготовку персонала правоохранительных органов, должна ли такая подготовка обеспечиваться производителями существующих средств криминалистики? Г-н Заврсник обратил внимание на то, что мы являемся свидетелями чрезмерно широкого распространения уголовного права, что в свою очередь может иметь серьезные последствия.

---

36 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/nickolov-modern-trends-sofia-oct-08.pdf.

37 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/zavrsnik-criminal-justice-system-sofia-oct-08.pdf.

67 Фредесвинда Инса, руководитель подразделения стратегического развития корпорации CYBEX, Испания, в своем представлении, озаглавленном "Необходимость создания европейской нормативно-правовой базы и обучения в сфере электронных доказательств"[38], конкретизировала необходимость разработки европейской нормативно-правовой базы и обучающих программ, касающихся обработки электронных доказательств. Она отметила, что новые технологии экспоненциально увеличили количество электронной документации в организациях всего мира, и теперь в мире ежегодно отправляется более 3 триллионов электронных сообщений. Исследования показывают, что во многих европейских организациях свыше 90 процентов документов являются электронными и лишь менее 30 процентов из них печатаются. Использование цифровых средств и виртуальной среды не исключает возможность недобросовестного использования, и традиционные доказательства постепенно переходят с бумажных носителей и печати в виртуальную среду. В условиях существования электронных доказательств процедуры управления и критерии приемлемости изменяются. Электронные доказательства приобретают все большую значимость в судебных процедурах, поскольку они являются наилучшим способом доказательства того, что некоторые виды преступлений были совершены с использованием этих технологий, сказала она. Тем не менее существующее законодательство в европейских странах, которые были обследованы, не содержит какого-либо конкретного определения электронных доказательств и не регулирует порядок их обработки.

68 Г-жа Инса отметила, что результаты соответствующего исследования, которое Cybex, испанская организация, занимающаяся изъятием, анализом и представлением электронных доказательств в суды, провела среди европейских судей, адвокатов, прокуроров и правоохранительных органов, выявило необходимость разработки европейской нормативно-правовой базы и обучающих программ, касающихся электронных доказательств. С учетом переходного характера электронных доказательств, они должны помочь странам разработать свои национальные законодательства в этой области и в то же время обеспечить стандартизированный подход на региональном и международном уровнях при обработке электронных доказательств. Вот почему в настоящее время обсуждаются конкретные процедуры получения, анализа и представления электронных доказательств, продолжала г-жа Инса. В европейских странах, которые были обследованы, к электронным доказательствам применяются общие процессуальные действия, хотя иногда применяются также процессуальные действия, предусмотренные для традиционных доказательств. К тому же в отдельных странах требования законодательств иногда не учитывают такие факторы, как: вопросы, касающиеся основных прав и защиты данных, существующие законы об электросвязи, система охраны вещественных доказательств при их передаче, меры, касающиеся достоверности доказательств и т. д. Г-жа Инса завершила свое представление информацией о некоторых проектах, реализуемых в настоящее время на европейском уровне и касающихся электронных доказательств. Что касается обучения в области электронных доказательств, то она предоставила информацию о новой программе "Европейский сертификат, касающийся киберпреступности и электронных доказательств", имеющей целью подготовку судей, прокуроров и адвокатов. Эта программа будет реализована с участием 13 европейских стран, а также Аргентины, Бразилии и Венесуэлы, в рамках академических программ и затем распространена на семинары и курсы. Г-жа Инса отметила также, что вскоре начнет работать первая электронная библиотека по электронным доказательствам и киберпреступности, содержащая правообразующие документы, судебные прецеденты, статьи экспертов и т. д., и полным ходом ведется подготовка электронного бюллетеня по электронным доказательствам и борьбе с киберпреступностью.

69 Андреа Джирардини, консультант и эксперт в области компьютерной криминалистики Межрегионального научно-исследовательского института Организации Объединенных Наций по вопросам преступности и правосудия, в своем представлении на тему "Открытое программное обеспечение применительно к компьютерной криминалистике"[39] рассмотрел вопросы компьютерной криминалистики и открытого программного обеспечения, заострив внимание на операционной системе GNU/Linux. Открытое программное обеспечение, сказал г-н Джирардини, должно использоваться в компьютерной криминалистике по нескольким соображениям. Некоторые неопровержимые доводы включают необходимость уменьшения затрат, что крайне желательно для стран с формирующейся экономикой и стран с небольшим целевым бюджетом, а также обеспечения

---

38 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/insa-cyber-forensics-sofia-oct-08.pdf.

39 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/ghirardini-open-software-sofia-oct-08.pdf.

возможности использования технологий, которые могут функционировать более эффективно по сравнению с коммерческими решениями. Кроме того, открытое программное обеспечение обновляется быстрее по сравнению с коммерческим программным обеспечением, что имеет важное значение для области, вынужденной быстро развиваться в связи с изменениями, происходящими в области технологий. Г-н Джирардини отметил также некоторые другие преимущества, связанные с использованием открытого программного обеспечения при проведении криминалистического анализа, с точки зрения его готовности (это программное обеспечение имеется в сети и его старая версия также может быть найдена), открытого формата (файлы могут быть легко преобразованы из одного формата файла в другой), возможности повторной проверки проведенного анализа (другие участники могут проверить каждый этап анализа), а также прозрачности (открытое программное обеспечение можно легко проверить).

Заседание 9: Экономика кибербезопасности

70 Слабые места в системе безопасности часто являются следствием порочных стимулов, а не отсутствия подходящих механизмов технической защиты. Поскольку отдельные лица и компании не несут всех затрат, связанных с киберинцидентами, то они не стремятся защитить свои системы наиболее эффективным способом. Если бы они несли все финансовые последствия, то у них были бы более весомые стимулы сделать свои сети более безопасными, что отвечало бы интересам всех присоединяемых сетей. На заседании 9 форума были рассмотрены основные современные идеи и научные разработки в области экономики кибербезопасности и было представлено последнее исследование МСЭ, посвященное Финансовым аспектам сетевой безопасности: вредоносные программы и спам[40]. Румен Трифонов, секретарь Координационного совета по вопросам информационного общества при Совете министров Болгарии, выполнял функции ведущего заседания 9, выступил со вступительным словом и руководил последующей дискуссией.

71 Мишель ван Этен, доцент школы технологий, политики и управления Дельфтского технического университета Нидерландов, представил анализ "Исследования МСЭ, касающегося финансовых аспектов сетевой безопасности: вредоносные программы и спам"[41]. Исследование представляет собой обзор существующих ресурсов и имеющихся данных по экономическим и финансовым аспектам кибербезопасности. Меры по повышению информационной безопасности повышают доверие к онлайновым операциям и прямо или косвенно способствуют повышению благосостояния, связанного с использованием информационно-коммуникационных технологий (ИКТ), пояснил г-н ван Этен. Однако необходимо понести лишь некоторые затраты, вследствие неослабевающих атак со стороны мошенников и киберпреспупников, подрывающих доверие к онлайновым транзакциям и представляющих для них угрозу. Такие затраты не повышают благосостояние, а, напротив, ложатся бременем на общество. Эти атаки совершаются в основном двумя способами: посредством вредоносных программ и спама. За прошедшие два десятилетия производство и распространение вредоносных программ переросло в бизнес стоимостью во многие миллиарды долларов. Ущерб, причиненный в результате мошеннической и преступной деятельности, основанной на использовании вредоносных программ, и затраты по принятию превентивных мер, по-видимому, значительно превышают эту величину. Вредоносные программы представляют угрозу для частного и государственного секторов, поскольку они все в большей степени рассчитывают на чистый доход от информационных услуг, сказал он.

72 Спам и вредоносные программы влекут за собой многоаспектные финансовые последствия для затрат и доходов участников в цепочке создания стоимости в сфере ИКТ. Они прямо или косвенно влияют на затраты, которые ложатся на все заинтересованные стороны по всей сети создания стоимости информационных услуг. При этом о большей части финансовых потоков между законными и незаконными участниками теневой экономики киберпреступности известно лишь частично. Базовое исследование, подготовленное г-ном ван Этеном и его командой, очерчивает рамки, в пределах которых могут быть оценены эти финансовые последствия, и сводит воедино многочисленные разрозненные источники финансовых данных, касающихся вредоносных программ и спама. Некоторые из выводов этого отчет включают: a) оценки финансовых последствий вредоносных программ сильно отличаются, данные в отношении суммарного воздействия,

---

40 http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf.

41 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/eeten-financial-aspects-sofia-oct-08.pdf.

располагаются в диапазоне от 13,2 млрд. долларов США прямого ущерба глобальной экономике (в 2006 г.) до 67, 2 млрд. долларов США прямого и косвенного влияния на бизнес в одних только США (в 2005 г.); b) цифры, подтверждающие масштабы теневой экономики интернета и транзакций между ней и формальной экономикой, также значительно отличаются. Один из источников оценивает размеры всемирной теневой экономики в 105 млрд. долларов США; c) в настоящее время достоверных данных о потенциальных издержках от неиспользованных возможностей для общества в целом в результате падения доверия не существует, однако значительное число пользователей указало на то, что оно снижает их готовность осуществлять онлайновые транзакции; d) несмотря на то что документальных подтверждений финансовых аспектов вредоносных программ и спама становится все больше, существующая информация страдает серьезными пробелами и противоречиями. Это осложняет поиск целенаправленных и эффективных ответных мер, и поэтому было бы крайне желательно предпринимать систематические усилия по сбору более достоверной информации, пояснил г-н ван Этен.

Заседание 10: Региональное и международное сотрудничество

73 Региональное и международное сотрудничество чрезвычайно важно для поддержания национальных усилий и содействия взаимодействию и взаимообмену. Проблемы, связанные с кибератаками и киберпреступностью, имеют глобальные и далеко идущие последствия, и эти проблемы могут быть решены только путем реализации согласованной стратегии в рамках международного сотрудничества с учетом ролей различных заинтересованных сторон и существующих инициатив. В качестве содействующей организации для Направления деятельности C5 ВВУИО, посвященного укреплению доверия и безопасности при использовании ИКТ, МСЭ обсуждает с ключевыми заинтересованными сторонами вопрос о том, как эффективнее реагировать на эти растущие проблемы кибербезопасности скоординированным образом. Так, например, Глобальная программа кибербезопасности МСЭ (GCA) предоставляет платформу для установления диалога, направленного на максимально эффективную реализацию существующих инициатив и развитие сотрудничества с признанными источниками специальных знаний в целях разработки глобальных стратегий для укрепления доверия и безопасности в информационном обществе. На заседании были рассмотрены некоторые из реализуемых в настоящее время инициатив, для того чтобы информировать участников форума и способствовать развитию дискуссий, с целью определения возможных последующих шагов и конкретных мер для поддержания и дальнейшего развития международного сотрудничества, направленного на усиление кибербезопасности.

74 Марко Обисо, Советник Отдела приложений ИКТ и кибербезопасности Сектора развития электросвязи МСЭ (МСЭ-D), открыл заседание представлением о деятельности МСЭ по международному сотрудничеству в целях обеспечения более безопасного киберпространства "Анализ Глобальной программы кибербезопасности МСЭ"[42]. Он отметил, что GCA МСЭ прокладывает путь к более широкому глобальному сотрудничеству в целях обеспечения более безопасного и защищенного киберпространства. Насчитывая 191 Государство-Член и свыше 700 Членов Секторов, включающих ведущих представителей отрасли, МСЭ как никто другой призван служить форумом для международного сотрудничества в области кибербезопасности. Учитывая богатый опыт МСЭ в области кибербезопасности, мировые лидеры, собравшиеся на Всемирной встрече на высшем уровне по вопросам информационного общества, поручили ему взять на себя лидирующую роль по Направлению деятельности C5, посвященному укреплению доверия и безопасности при использовании ИКТ, продолжал г-н Обисо. Таким образом, МСЭ через свои Сектора, МСЭ-R, МСЭ-T и МСЭ-D, вырабатывает глобальный, скоординированный и согласованный подход к вопросам обеспечения кибербезопасности. Г-н Обисо отметил, что МСЭ, как ведущая содействующая организация по Направлению деятельности C5 ВВУИО, работает со всеми основными заинтересованными сторонами над тем, как эффективнее и скоординированным образом реагировать на растущие проблемы кибербезопасности. В этом отношении Глобальная программа кибербезопасности МСЭ может предложить стратегические направления, которые должны стимулировать дальнейшее развитие международного сотрудничества. Он упомянул также ведущую роль, которую сыграли Сектора МСЭ, в частности МСЭ-D, в преобразовании согласованных стратегий в конкретные действия и проекты, которые будут реализованы вместе с партнерами в странах Европы и СНГ, а также в других регионах.

---

42 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/obiso-GCA-overview-sofia-oct-08.pdf.

75 После этого старший эксперт по связям с отраслью и международными организациями ENISA, г-н Илари Патрик Линди, представил краткий обзор деятельности ENISA в области регионального и международного сотрудничества, содержащийся в "ENISA и региональное сотрудничество"[43]. ENISA было создано, согласно своего регламента, в качестве стимулирующего органа и катализатора для работы над элементами, обеспечивающими бесперебойное функционирование рынка, а не для реализации политики в области европейской безопасности или координации сотрудничества полицейских сил. Имея в своем составе 30 оперативных сотрудников, ENISA работает также над повышением общего уровня сетевой и информационной безопасности европейских государств-членов и, в целом, в качестве содействующей организации в создании зоны более прочного европейского сотрудничества. Для обеспечения более активного участия заинтересованных сторон нам необходимо знать, в чем нуждаются заинтересованные стороны, какие барьеры существуют на рынке и какие там могут быть стимулы, продолжал он. ENISA выступает в качестве посредника между государствами-участниками в области сетевой и информационной безопасности и работает над объединением различных заинтересованных сторон и групп заинтересованных сторон в регионе, используя различные пропагандистские инструменты и средства коммуникации, для того чтобы заинтересованные стороны были лучше осведомлены о предпринимаемой деятельности.

76 Далее г-н Линди отметил, что заинтересованные стороны стран, не входящих в Европейский союз, также проявляют большой интерес к деятельности ENISA. В настоящее время ENISA работает в основном с теми странами, в которых могут быть реализованы совместные инициативы в области исследований, сказал он. ENISA можно рассматривать также в качестве организационной модели, объединяющей многие самые различные страны, представителей из самых различных сфер, совместно работающих над инициативами в области сетевой и информационной безопасности, сказал он. ENISA не стремится создавать документы, а хочет понять, как различные подходы реализуются на практике в соответствующих странах, продолжил г-н Линди.

77 После этого Александр Донос, директор государственного предприятия Центра специальной связи Молдовы и председатель Комиссии по информационной безопасности при Координационном совете Регионального содружества в области связи (РСС), представил краткий обзор "Деятельности Комиссии по информационной безопасности при Координационном совете Государств – Членов СНГ по информатизации при РСС"[44]. Он отметил, что основные цели и функции Комиссии включают, в частности: разработку рекомендаций в области информационной безопасности; обмен информацией и опытом в создании систем и средств обеспечения информационной безопасности систем и сетей информации и электросвязи; подготовку совместных предложений и определение приоритетности вопросов для стран СНГ; подготовку совместных рекомендаций, касающихся разработки межгосударственных программ в области информационной безопасности; разработку предложений по гармонизации национальных законодательств в Государствах – Членах СНГ; и подготовку предложений по дальнейшему развитию рынка. Г-н Донос поделился также подробными сведениями о пилотном проекте по трансграничному обмену юридически важной информацией с применением цифровой подписи в 2009–2011 годах, организуемом по результатам совместной научно-исследовательской работы РСС на тему "Исследование возможности использования электронно-цифровой подписи при трансграничном информационном обмене".

78 Мэтью Ламберти, координатор по вопросам обеспечения соблюдения действующего законодательства в области интеллектуальной собственности для Восточной Европы Департамента юстиции США, посольство Соединенных Штатов Америки в Болгарии, сделал представление о "Содействии развитию регионального и международного сотрудничества по вопросам кибербезопасности"[45] и сети 24/7 на случаи преступлений в сфере высоких технологий, изначально являющейся инициативой G8, – сети, которая обеспечивает контактную сеть для сообщений о проблемах, связанных онлайновой преступностью. Эта сеть имеет целью обеспечить простой механизм сотрудничества, который может использоваться странами для сообщения об инцидентах и принятия соответствующих мер. Эта сеть состоит из представителей правоохранительных органов,

---

43 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/lindy-regional-cooperation-sofia-oct-08.pdf.

44 http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/donos-RCC-overview-sofia-oct-08.pdf.

45 Слайды отсутствуют.

которые, помимо прочего, обмениваются информацией и советом в отношении защиты данных, контактов с ISP, а также о том, как начать процесс оказания взаимной юридической помощи. Эта сеть открыта для всех стран и в нее легко войти. Единственное требование заключается в том, чтобы соответствующая страна определила контактное лицо для вызова, обладающее достаточными техническими знаниями на случай, когда речь зайдет о киберпреступлениях, поскольку одной из основных задач, связанных с этими случаями киберпреступности, является обработка цифровых судебных доказательств. Это лицо должно быть также знакомо с внутренним законодательством и процедурами, касающимися электронных доказательств. Использование этого инструмента доказало свою эффективность, продолжал г-н Ламберти, и привел ряд примеров, когда данная сеть предоставляла информацию, позволившую выявить и арестовать киберпреступников.

79 Эдуард Джансериков, руководитель сектора информационной безопасности ОАО, Кыргызтелеком, Кыргызская Республика, в своем выступлении рассмотрел тему "Сотрудничество операторов электросвязи стран – участниц РСС в области кибербезопасности"[46]. Г-н Джансериков отметил, что координация деятельности в области кибербезопасности в странах РСС в настоящее время осуществляется с участием соответствующих представителей частного сектора. Он ознакомил участников с примерами некоторых видов деятельности, предпринятой объединениями частного сектора РСС, в целях содействия развитию международного сотрудничества. Далее г-н Джансериков подчеркнул важность установления и поддержания связей между представителями частного сектора и соответствующими правительственными учреждениями, а также с международными организациями.

80 После этого выступил Ярослав Пондер, координатор для Европы, Сектор развития электросвязи МСЭ (МСЭ-D), обративший внимание участников на регулярную разработку программ деятельности МСЭ-D в области кибербезопасности и способы реагирования на потребности стран в регионе в этом отношении. Он упомянул также предстоящую Всемирную конференцию по развитию электросвязи (ВКРЭ)[47], которая должна состояться в 2010 году, и проинформировал о том, как Государства-Члены могут активно участвовать в этой Конференции и подготовительной работе к ней. Г-н Пондер подчеркнул важность активного участия всех администраций в работе Региональных подготовительных собраний, которые будут проходить в 2009 году. Эти подготовительные собрания предоставляют прекрасную возможность для определения потребностей стран на региональном уровне, в том числе в области кибербезопасности.

Заседание 11: Подведение итогов, рекомендации и дальнейшие действия

81 Вести заключительное заседание собрания помогали Красимир Симонски, заместитель председателя Государственного агентства информационных технологий и связи (SAITC), Болгария, и Марко Обисо, Советник Отдела приложений ИКТ и кибербезопасности Бюро развития электросвязи МСЭ (МСЭ-D). Они подвели основные итоги данного мероприятия и разработали ряд рекомендаций в отношении будущей деятельности в целях повышения кибербезопасности и защиты важнейших информационных инфраструктур в регионе. Были сформулированы некоторые рекомендации для принятия конкретных действий странами региона.

82 Г-н Обисо отметил необходимость для стран принятия действий в целях:

- Анализа и, в случае необходимости, пересмотра существующего или подготовки нового законодательства, для того чтобы криминализовать ненадлежащее использование ИКТ с учетом быстро развивающихся угроз кибербезопасности. Этот процесс должен будет учитывать: 1) требования в связи с атаками и угрозами, возникающими в различных странах; 2) требования в связи с атаками или угрозами, возникающими извне и представляющими угрозу для той или иной страны. Эти два требования могут быть трансформированы в эффективный механизм, если принять во внимание международные механизмы. Должно быть разработано национальное законодательство, а законы в области кибербезопасности приведены в соответствие с существующими международными инструментами.

---

[46] Слайды отсутствуют.

[47] http://www.itu.int/ITU-D/wtdc/.

- Разработки необходимых организационных структур для эффективного решения вопросов, связанных с кибербезопасностью. Этот процесс должен предусматривать создание структуры, отвечающей за вопросы кибербезопасности в конкретной стране. Эта структура может принадлежать непосредственно правительству или работать в тесном сотрудничестве с ним. Отдельные возможные компоненты такой структуры могут включать:
  - национального координатора по вопросам кибербезопасности (отдельное лицо или службу), в задачу которого будет входить организация работы и координация усилий, взаимодействие с правительством, представителями деловых кругов и научного сообщества;
  - возможности по устранению инцидентов с ответственностью на государственном уровне. Эта деятельность должна включать возможное создание Национального центра кибербезопасности с целью учреждения в среднесрочной/долгосрочной перспективе CERT/CSIRT.
- Включения в текущую деятельность в области кибербезопасности страны мер по усилению защиты детей. Это предполагает создание технических механизмов, ставящих своей целью уменьшение рисков для детей и молодежи, работающих в онлайновом режиме, включая:
  - разработку механизмов аутентификации и авторизации для обеспечения защиты детей от неподобающего материала;
  - разработку международно признанной базы данных для правоохранительных органов.
- Обеспечения скоординированных усилий в нескольких областях, относящихся к сфере криминалистики и анализу кибербезопасности, включая:
  - профессиональную подготовку и создание потенциала;
  - экономически эффективные технические решения для осуществления деятельности в области криминалистики.

83 Далее г-н Симонски отметил необходимость для стран:

- Приобретения опыта и специальных знаний, являющихся важными компонентами для развития потенциала в области кибербезопасности и обмена знаниями. Повышение осведомленности и профессиональная подготовка были отмечены в качестве основных элементов усилий стран по созданию потенциала в области кибербезопасности.
- Объединения различных заинтересованных сторон в области кибербезопасности и создания платформы для развития партнерских отношений в целях повышения кибербезопасности. Определение соответствующих игроков в сфере кибербезопасности и налаживание диалога в целях установления возможных партнерских отношений и создания механизмов эффективного сотрудничества имеют решающее значение для дальнейшего продвижения вперед. Тесное сотрудничество и взаимный обмен опытом позволят лучше понять деятельность, роль и компетенции каждой из сторон.
- Разработки справедливой основы для реализации подхода, основанного на участии многих заинтересованных сторон. Присутствие различных участников и игроков должно быть гарантировано, что позволит обеспечить учет многочисленных точек зрения. Должна быть проведена конкретная работа, исходя из перспектив и аспектов, характеризующих функциональную среду кибербезопасности, с учетом ролей соответствующих заинтересованных групп:
  - бизнеса − для обеспечения включения в процесс последних технических разработок;
  - правительства − для обеспечения общей подотчетности и ответственности. Важно, чтобы государственный сектор играл активную роль в целях обеспечения стабильности и непрерывности при защите важнейшей информационной инфраструктуры;
  - международных и межправительственных организаций − для обеспечения учета международного сотрудничества и глобального аспекта реакций, связанных с кибербезопасностью. Лишь НПО могут рассматривать вопросы международной государственной политики и определять механизмы, которые могут повести процесс в направлении глобальной кибербезопасности. В частности, МСЭ, в рамках своей Глобальной программы кибербезопасности и с учетом его роли ведущей содействующей организации по Направлению деятельности С5 ВВУИО, является ключевым игроком, с которым соответствующий правительственный орган может работать в этом отношении.

84 Г-н Симонски подчеркнул, что Болгария воспользуется специальными знаниями МСЭ, для того чтобы получить надлежащую помощь в процессе разработки национальной политики в области кибербезопасности в четко установленных рамках международного сотрудничества.

Закрытие собрания

85 В своих заключительных замечаниях от имени МСЭ Марко Обисо, Советник Отдела приложений ИКТ и кибербезопасности Бюро развития электросвязи МСЭ (МСЭ-D), выразил надежду на то, что трехдневный Региональный форум по кибербезопасности для стран Европы и СНГ оказался полезным для всех участников данного мероприятия. Г-н Обисо поблагодарил всех тех, кто прямо или косвенно способствовал успешному проведению Регионального форума по кибербезопасности, и выразил особую признательность местным организаторам за их выдающуюся работу, позволившую обеспечить успех данного мероприятия. Г-н Обисо поблагодарил ораторов форума, которые выбрали время в своем загруженном рабочем графике, для того чтобы приехать и поделиться опытом и специальными знаниями с участниками форума. МСЭ, который уже длительное время занимается деятельностью в области стандартизации и развития электросвязи, надеется и впредь предоставлять форум, в рамках которого можно будет обсудить различные точки зрения между представителями правительственных учреждений, частного сектора и других заинтересованных сторон, по вопросам кибербезопасности и CIIP, исходя из его различных видов деятельности и инициатив.

Ниже приводится адрес электронной почты для направления замечаний по отчету о данном собрании[48], а также для замечаний по программе работы МСЭ в области кибербезопасности в помощь развивающимся странам (2007–2009 гг.)[49]: cybmail(at)itu.int[50].

В целях совместного использования информации все участники собрания будут добавлены в cybersecurity-europe-cis(at)itu.int[51] для вопросов, касающихся деятельности МСЭ-D в области кибербезопасности. Если вы не принимали непосредственное участие в данном мероприятии или еще не включены в список рассылки, но заинтересованы в участии в дискуссиях посредством соответствующего списка рассылки и форума, то направьте электронное сообщение по адресу: cybmail(at)itu.int.

---

48 Данный отчет о работе Форума доступен в сети по адресу: http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/sofia-cybersecurity-forum-report-oct-08.pdf.

49 http://www.itu.int/ITU-D/cyb/cybersecurity/index.html#workprogramme.

50 Направьте, пожалуйста, любые замечания, которые у вас могут возникнуть по данному отчету о работе Форума, по адресу: cybmail@itu.int.

51 Региональный список рассылки МСЭ, касающийся вопросов кибербезопасности: cybersecurity-europe-cis@itu.int. Направьте, пожалуйста, электронное сообщение по адресу: cybmail@itu.int, чтобы его можно было добавить в список рассылки.