Координационная конференция Октопус

Сотрудничество против киберпреступности

Совет Европы, Страсбург, Франция, 11 – 12 июня 2007 года

Резюме конференции

С 11 по 12 июня 2007 года в Совете Европы в Страсбурге состоялась встреча более 140 экспертов в области киберпреступности, представляющих около 55 стран, международных организаций и частный сектор, для того чтобы:

- проанализировать угрозу киберпреступности;
- провести обзор эффективности законодательства в сфере киберпреступности;
- содействовать применению Конвенции о киберпреступности и Протокола к ней как руководящих принципов для разработки национального законодательства и поощрять широкую и быструю ратификацию этих договоров и присоединение к ним;
- укреплять сотрудничество между разными инициативами посредством более эффективного использования существующих возможностей и поиска новых.

Итоги пленарных заседаний и обсуждений в рабочих группах:

1 КИБЕРПРЕСТУПНОСТЬ: АНАЛИЗ СИТУАЦИИ И ВЫЯВЛЕНИЕ НОВЫХ УГРОЗ

Проблемы

Доклад представителя Европола и последовавшая за ним дискуссия в рабочей группе с участием представителей Франции, компании Микрософт, Ассоциации Интернет-провайдеров «горячих линий» - INHOPE и Международного центра пропавших и эксплуатируемых детей - ICMEC, а также выступления других участников позволяют сделать следующие выводы:

- Общество во всем мире зависит от информационных и коммуникационных технологий. Рост киберпреступности делает эти общества весьма уязвимыми
- Вредоносные программные средства – вредоносные коды и программное обеспечение, включая вирусы, черви, трояны, программы-шпионы, боты и ботнеты, - все это развивается и распространяется весьма быстро и используется, помимо прочего, для атак типа "отказа в обслуживании", кражи имени (фишинг и другие методы социальной инженерии), мошенничества, отмывания денег и для совершения других экономических преступлений
- Спам, который занимает бóльшую часть трафика в электронной почте, не только вредит работе, но и все больше переносит вредоносные программные средства
- Правонарушители все больше организуются для совершения преступлений, направленных на извлечение незаконных доходов
- Одним из главных инструментов таких преступных организаций являются ботнеты, причем не только для атак типа "отказа в обслуживании" и вымогательства, но и для размещения адвэров и спайвэров

- Развивается экономика подпольных услуг, например, ботнеты арендуются представителями организованной преступности
- Серьезный сдвиг в "ландшафте угроз" подтверждается аналитиками из промышленности: широкие, массированные, многоцелевые и даже глобальные атаки вирусами, червями и спамом, которые привлекают всеобщее внимание, сейчас заменяются более целенаправленными, маломасштабными атаками на конкретных пользователей, группы, организации или сектора, и при этом ставится цель избежать привлечения внимания. Такие атаки все чаще преследуют цели совершения экономических преступлений
- Особо уязвимы - малые и средние предприятия, поскольку зачастую они не вкладывают необходимых средств в защиту своих систем
- Системы виртуальной оплаты он-лайн становятся серьезной проблемой в США
- Интернетом злоупотребляют в целях сексуальной эксплуатации и насилия в отношении детей и для торговли людьми. Большая часть сайтов с детской порнографией и кадрами с актами насилия над детьми имеют коммерческий характер и приносят большие доходы
- Растет риск кибератак в отношении важнейших инфраструктур (кибертерроризм)
- Дистанционное хранение данных создает проблемы в отношении расследования киберпреступлений
- Технологии и методы совершения киберпреступлений развиваются быстрыми темпами и становятся все более изощренными. Сети следующего поколения (ССП), включая такие услуги, как голосовые сообщения по IP, вызывают новые угрозы правопорядку.

Перспективы

Были выдвинуты, в том числе, следующие предложения:

- В борьбе с киберпреступностью необходимо всемирное сотрудничество. Страны мира должны поддержать всемирные стандарты как основу для обмена информацией. Важным шагом в этом направлении будет как можно более полная реализация Конвенции о киберпреступности
- Партнерство между государством и частным сектором является краеугольным камнем такого всемирного сотрудничества. Промышленность несет большую ответственность за сотрудничество с правоохранительными органами. Задача состоит в том, чтобы найти правильный баланс между правом на частную жизнь и задачами обеспечения безопасности
- Содействовать тому, чтобы жертвы киберпреступности сообщали об этих фактах; способствовать передаче таких обращений и принимать меры по защите свидетелей
- Совершенствовать качество и координацию данных о киберпреступности, например, через централизованные системы обращений, поиск кибернарушителей и прочее
- Не только государственные органы, но и промышленность и другие организации частного сектора должны продолжать свою важнейшую работу по оценке угроз и проведению анализа. Например, предстоящий доклад INHOPE о тенденциях в области детской порнографии и незаконного содержания даст полезную информацию в этой области
- Установление уголовной ответственности за детскую порнографию и насилие над детьми в Интернете будет означать полное выполнение статьи 9 Конвенции о киберпреступности, без каких-либо оговорок, если только это абсолютно необходимо

- Следует выполнять также и другие договоры и правовые нормы по защите детей от насилия
- Улучшать образование для безопасного пользования информационно-коммуникационными технологиями на всех уровнях, например, на основе специализированных программ или учебных учреждений. Сами пользователи (индивидуальные пользователи, а также компании и государственные органы) несут огромную ответственность за предупреждение и собственную защиту
- Осуществлять меры по защите важных инфраструктур
- Предпринимать шаги по нахождению решений в отношении тех вызовов, которые связаны с такими технологическими разработками, как сети следующего поколения, включая голосовые сообщения по IP.

2 ВЫПОЛНЕНИЕ КОНВЕНЦИИ О КИБЕРПРЕСТУПНОСТИ И ПРОТОКОЛА О КСЕНОФОБИИ И РАСИЗМЕ

Проблемы

Киберпреступность - широкое явление, которое быстро растет и становится все более опасным, пересекая границы без каких-либо трудностей. Совершенно ясно, что с ним нужно и можно бороться во всемирных масштабах. Для этого страны должны иметь не только совместимое, но и – возможно в бóльшей степени - согласованное материальное и процессуальное уголовное законодательство, но также осуществлять всю деятельность в более тесном контакте для обеспечения эффективного международного сотрудничества.

Конвенция о киберпреступности предоставляет собой практические и получившие одобрение основные направления деятельности по развитию национального законодательства и создает рамки для международного сотрудничества. На настоящий момент Конвенцию ратифицировало 21 государство и подписало 22. Дополнительный протокол о расизме и ксенофобии был ратифицирован 11 государствами и подписан еще 20.

Проблемы включают:

- расширение круга участников Конвенции и Дополнительного протокола, в частности, те государства, которые уже подписали эти договоры, должны ускорить процесс ратификации;
- продвижение Конвенции во всемирном масштабе. В дополнение к шести неевропейским государствам, которые подписали или ратифицировали этот договор или которым было предложено к нему присоединиться, необходимо поощрять и другие государства сделать это;
- обеспечение и повышение эффективности Конвенции и Дополнительного протокола к ней между сторонами.

Обмен передовой практикой

Учитывая важность Конвенции, которая является единственным международным договором по киберпреступности в мире, ее положения часто используются как модель для проектов законов. Благодаря такой широкой поддержке Конвенции в разных регионах мира практически все новое законодательство или законопроекты тесно связаны с положениями Конвенции. Эти реформы в настоящее время осуществляются, например, в таких странах, как Аргентина, Бразилия, Египет, Индия, Нигерия, Пакистан и Филиппины.

Это обеспечивает во всемирных масштабах совместимость законов и создает прочную и эффективную основу для совместной работы между странами.

Перспективы

- Страны, которые уже подписали Конвенцию или Протокол или которым предложено присоединиться к ним, должны как можно скорее завершить процесс ратификации
- Те страны, которые выполняют Конвенцию, должны делиться своим опытом. В этом отношении может быть полезен такой документ, как "Информация о законодательстве в области киберпреступности по странам", подготовленный в Совете Европы в рамках проекта по киберпреступности[1]
- Совет Европы и другие партнеры готовы оказывать содействие заинтересованным странам и консультировать их по законодательству в сфере киберпреступности
- Консультации Сторон - через Комитет по Конвенции о киберпреступности (T-CY) - обеспечат консультации и помощь в выполнении Конвенции и Протокола к ней.

3 ЭФФЕКТИВНОСТЬ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ КИБЕРПРЕСТУПНОСТИ

Проблемы

Страны должны ввести уголовную ответственность за определенные виды деяний (материальное уголовное право), обеспечить исполнение законов и уголовное правосудие средствами, позволяющими проводить эффективное расследование, преследовать правонарушителей и выносить судебные решения по киберпреступлениям (процессуальное право), включая необходимость быстро действовать для сохранения недолговечных доказательств, а также обеспечивать эффективное международное сотрудничество. Все страны призваны использовать в этом отношении Конвенцию как руководство к действию. Некоторые страны, которые уже являются участниками Конвенции, могут нуждаться также в том, чтобы осуществить дополнительные шаги по приведению своего законодательства в полное соответствие с этим договором.

Основная задача состоит в том, чтобы страны принимали национальное законодательство в области материального и процессуального уголовного права, а также осуществляли международное сотрудничество в соответствии с Конвенцией о киберпреступности.

Помимо этого, серьезную проблему для правоохранительных органов во всем мире представляет собой вопрос юрисдикции.

Обмен передовой практикой

Представители следующих государств проинформировали о своем внутреннем законодательстве в области киберпреступности и о связанных с этим вопросах: Италия, Румыния, Россия, Норвегия, Нидерланды, Португалия и

[1] См. www.coe.int/cybercrime.

Азербайджан, причем все они являются государствами - членами Совета Европы.
Также были представлены доклады следующими странами: Индия, Аргентина, Бразилия, Мексика, Египет и Южная Африка. В дополнение к этому представители компании Микрософт сделали обзор существующего законодательства в области киберпреступности и законодательных инициатив в государствах Азиатско-тихоокеанского региона.

Всеми были признаны и широко поддержаны преимущества Конвенции о киберпреступности и первого Дополнительного протокола к ней.

Большинство выступавших сделали обзор положений в существующем внутреннем законодательстве в области киберпреступности. Государства, подписавшие Конвенцию, и те государства, которые хотели бы к ней присоединиться, проинформировали о рассматриваемых законопроектах и дополнительных усилиях, которые будут предприняты в будущем в сфере законодательства. Можно сделать вывод о том, что в большинстве случаев реализация положений Конвенции привела к серьезному пересмотру существующих и принятию новых законов. Из предоставленной информации можно сделать вывод и о том, что в 2007 году следует ожидать значительного количества ратификаций, а также обращений с просьбой о присоединении к Конвенции.

Отмечался ряд сложных моментов, с которыми сталкиваются законодатели в странах при реализации текста Конвенции, в частности в отношении статьи 2 (незаконный доступ), статьи 3 (незаконный перехват), статьи 9 (детская порнография), статьи 32 (трансграничный доступ) и статьи 35 (24/7). Кроме того, ряд выступавших - включая тех, кто уже подписал или ратифицировал Конвенцию, - говорили о конкретных формах киберпреступности, в отношении которых в рамках национального законодательства установлена уголовная ответственность, но которые не являются (специально) оговоренными Конвенцией, такие, как кража личной информации, киберпреследование и кибердиффамация. Для последующей работы по установлению уголовной ответственности необходимо изучить такие формы ИКТ, как Wifi, биометрическая идентификация, радиометки (RFID).

Был поднят ряд проблем, связанных со сбором электронных улик, в частности улик, находящихся вне национальной территории. В Конвенции предусматривается ускоренное оказание взаимопомощи для сохранения электронных улик на территории другой страны.
Возникли трудности в сотрудничестве между государствами - членами Совета Европы и государствами-нечленами. Например, обычные процедуры Многосторонних соглашений (MLA) для передачи запрашиваемого материала в целом занимают достаточно много времени, что может затруднить расследование и наказание в связи с преступлениями. Помимо этого, говорилось о том, что существуют трудности при определении физического расположения компьютерного сервера, что мешает правоохранительным органам обращаться с просьбами о взаимной помощи.

Кратко был обсужден вопрос о том, что необходимо обеспечить принудительные меры для того, чтобы заставлять Интернет-провайдеров (ISP) блокировать трафик в Интернете, который исходит из определенных источников, с учетом его содержания. В некоторых странах такие возможности предусмотрены, в других случаях блокирование осуществляется в сотрудничестве с Интернет-провайдерами.

Большинство представителей подчеркивали необходимость проведения специализированных расследований и наличия координирующих органов на национальном уровне, а также постоянного обучения и профессиональной подготовки, особенно для сотрудников прокуратуры и судебных органов.

Некоторые представители привлекли внимание к тому, что в их странах с развивающейся экономикой могут отсутствовать достаточные средства для предоставления правоохранительным органам и судебной системе необходимого оборудования и экспертизы. Необходима поддержка со стороны других государств и частного сектора.

В заключение сессии были изложены подробности процедуры и условий присоединения к Конвенции и последующей ратификации.

Перспективы

- Возможно, существует необходимость в проведении более тщательной оценки эффективности законодательства в сфере борьбы с киберпреступностью, а также обмена передовой практикой. Этому может способствовать подготовленный Советом Европы документ "Информация о законодательстве в области киберпреступности по странам"
- Страны, которые в настоящее время находятся на этапе подготовки законодательства по борьбе с киберпреступностью, могут запрашивать Совет Европы и власти стран - участниц Конвенции, а также частный сектор о помощи в подготовке законодательства по киберпреступности
- Следует укреплять возможности уголовного правосудия и правоохранительных органов по исполнению законов в сфере киберпреступности
- Вопрос о юрисдикции может быть дополнительно рассмотрен на соответствующей площадке, в том числе и на Комитете Конвенции о киберпреступности (T-CY).

4 МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО И ФУНКЦИОНИРОВАНИЕ СЕТЕЙ КОНТАКТНЫХ ПУНКТОВ 24/7

Проблемы

Киберпреступность является международным видом преступности, что подразумевает необходимость эффективного и неотложного международного сотрудничества для сохранения недолговечных улик. В этом отношении важным инструментом является сеть контактных пунктов, работающих 24 часа в сутки семь дней в неделю. За создание таких контактных пунктов выступает Подгруппа по преступности в сфере высоких технологий Большой восьмерки начиная с 1997 года, и это же предусматривается в статье 35 Конвенции о киберпреступности.

Встают следующие проблемы:

- Не все Стороны в Конвенции создали действующие контактные пункты
- Риск наличия разных сетей контактных пунктов, например, в рамках Большой восьмерки и в рамках Совета Европы
- В ряде стран не полностью обеспечена юридическая основа для контактных пунктов (например, в отношении срочного сохранения данных)
- Необходимость содействовать сотрудничеству между контактными пунктами благодаря эффективному сотрудничеству судебных органов

Передовая практика

Значительный опыт накоплен в рамках сети Подгруппы по преступности в сфере высоких технологий Большой восьмерки за десять лет после ее создания. Группой подготовлены руководящие принципы и другая документация. "Протокольное заявление" может помочь странам создать контактные пункты. "Перечень для использования сети 24/7 Большой восьмерки" может помочь контактным пунктам сформулировать запросы в том формате, в котором содержится вся необходимая информация для действий того контактного пункта, к которому обращен запрос.
Были обсуждены примеры контактных пунктов в Италии, США, Франции и Румынии.

Перспективы

- В соответствии со статьей 35 все страны, ратифицировавшие Конвенцию, должны создать действующие контактные пункты. В случае необходимости члены сети Большой восьмерки и Совета Европы должны оказать поддержку в этом отношении.
- Контактные пункты, созданные на основании Конвенции, призываются также зарегистрироваться в сети Подгруппы по борьбе с преступностью в сфере высоких технологий Большой восьмерки.
- Подгруппа по борьбе с преступностью в сфере высоких технологий Большой восьмерки и Совет Европы должны сотрудничать для поддержания и обновления совместного Справочника по контактным пунктам (ограниченного целями правоохранительной деятельности). Это предложение должно быть обсуждено на следующем заседании подгруппы Большой восьмерки.
- Для облегчения сотрудничества между контактными пунктами было бы полезно иметь стандартизированные форматы для запросов, такие, как "Перечень для использования сети 24/7 Большой восьмерки"
- Италия планирует создать - при условии наличия средств - безопасный портал для использования сетью контактных пунктов. Это может помочь обновлять Справочник, а также обмениваться другой информацией, такой, как шаблоны для запросов
- После учебных конференций для контактных пунктов, организованных подгруппой Большой восьмерки в Риме, Италия, в 2004 и 2006 годах, можно предусмотреть еще одну учебную конференцию Большой восьмерки в 2009 году. Для сохранения динамики работы Совету Европы следует рассмотреть возможность организации учебного семинара для контактных пунктов уже в 2008 году
- Можно провести сетевые или пинг-тесты для проверки того, действуют ли контактные пункты
- Следует предпринять усилия по дальнейшему расширению сети. Это включает анализ состава, рабочих методов и полномочий уже существующих сетей в этой области, таких, как сеть Интерпола.

5 ИНИЦИАТИВЫ ДРУГИХ ОРГАНИЗАЦИЙ И УЧАСТНИКОВ: ВОЗМОЖНОСТИ ДЛЯ СОТРУДНИЧЕСТВА И ВЗАИМОДЕЙСТВИЯ

Проблема

В последние годы международные организации, государства, государственные и частные заинтересованные стороны осуществляли многочисленные проекты, которые свидетельствуют о решимости во всем мире бороться с киберпреступностью и искать необходимые решения. В результате этого

деятельность в этой сфере развивается весьма динамично, но существует серьезный риск дублирования (естественная тенденция работать обособленно и ограничивать координацию с другими). Все участники имеют единую и общую задачу, которая призывает к дальнейшей гармонизации и централизации усилий и действий, особенно на международном уровне. Такая координация должна действовать по принципу Интернета: ячейки соединяются друг с другом целесообразным образом, создавая синергетику и новую динамику. Встречи, подобные Конференции Октопус, в сочетании с официальной координацией между заинтересованными сторонами, могут стать интерфейсом для содействия такому сотрудничеству.

Обмен передовой практикой

Были представлены различные акции и программы, являющиеся передовой практикой, которой можно было бы обмениваться и которую следует и далее расширять, в частности в следующих областях: сотрудничество между правоохранительными органами и частным сектором в качестве общей платформы для обмена информацией и определения ролей и ожидаемого результата для каждого участника, при координирующей роли со стороны Европейской сети и Агентства по информационной безопасности (ENISA) с промышленностью, международными организациями, третьими странами и научными сообществами, а также проект Агентства по созданию Европейской системы обмена информацией и оповещения, ориентированной на граждан и малые и средние предприятия, набор мер и инструментов по противодействию распространению спама (Anti-spam Toolkit), подготовленный ОЭСР; Международная консультативная группа, созданная в рамках программы ЮНЕП по вопросам управления в регионе арабских государств (POGAR) для поддержки действий, направленных на подготовку в сфере уголовного правосудия в целях борьбы с преступностью в сфере высоких технологий; создание дополнительных горячих линий Интернета в Африке и Азии в рамках ассоциации INHOPE, которая содействует работе горячих линий в Интернете и координирует эту работу для реагирования на незаконное использование и содержание в Интернете; развитие глобальных кампаний против детской порнографии, аналогичных той, которая была развернута Международным центром по пропавшим без вести и эксплуатируемым детям.

Перспективы

Среди предложений по осуществлению совместных усилий и укреплению сотрудничества на международном уровне можно отметить:

- Форум по управлению в сфере Интернета: Совет Европы внесет свой вклад на следующем заседании в Рио-де-Жанейро (ноябрь 2007 года) и подчеркивает необходимость обеспечения того, чтобы Интернет был безопасным и чтобы в киберпространстве также соблюдались права человека и верховенство закона
- Такие организации, как Европейская организация по цифровым правам (European Digital Rights), будут продолжать наблюдать за тем, чтобы законы, направленные на борьбу с киберпреступностью, не ограничивали чрезмерно права на частную жизнь и свободу выражения мнения в Интернете
- Европейская Комиссия: сообщение Комиссии, опубликованное в мае 2007 года, может служить хорошей основой для дальнейшего сотрудничества. Комиссия выразила свою готовность содействовать Конвенции и Протоколу к ней, призывать третьи страны присоединиться к Конвенции и рассмотреть присоединение к Конвенции Европейских

Сообществ. Совет Европы готов принять участие в тех мероприятиях, о которых говорится в Сообщении

- Организация американских государств (ОАГ): и далее будет поддерживать присоединение своих государств-членов к Конвенции и готова рассмотреть дополнительные возможности сотрудничества с международными организациями. Совет Европы будет продолжать свое плодотворное сотрудничество с ОАГ и, возможно, рассмотрит проведение совместного учебного мероприятия по оказанию поддержки государствам - членам ОАГ в подготовке законодательства по киберпреступности
- Интерпол: призывает все свои государства-члены использовать инструменты (сеть 24/7, базы данных) в области преступности в сфере высоких технологий. Совет Европы готов поддержать встречи рабочих групп Ближнего и Среднего Востока, а также рабочей группы Африки в конце 2007 года
- Азиатско-тихоокеанское экономическое сотрудничество и АСЕАН: будут и далее продвигать Конвенцию среди своих государств-членов и укреплять законодательство по киберпреступности. Совет Европы готов работать через АТЭС и АСЕАН со странами Азии и тихоокеанского бассейна для достижения этой цели, а также готов внести свой вклад в следующее заседание рабочей группы АТЭС ТЕЛ в Чили соответствующим образом
- Организация Исламская конференция (ОИК): продолжит свою деятельность по борьбе с диффамацией религии в Интернете. Совет Европы должен сотрудничать с ОИК для борьбы против нетерпимости и дискриминации на основе Конвенции о киберпреступности и Дополнительного протокола к ней, касающегося установления уголовной ответственности за акты расизма и ксенофобии
- ЮНЕП POGAR: Совет Европы внесет свой вклад в следующую учебную конференцию для прокуроров из арабских стран по киберпреступности, организованную ЮНЕП POGAR в Касабланке 19-20 июня 2007 года. Можно рассмотреть и дальнейшее сотрудничество между Советом Европы и ЮНЕП POGAR.

6 ПАРТНЕРСКИЕ СВЯЗИ МЕЖДУ ГОСУДАРСТВЕННЫМ И ЧАСТНЫМ СЕКТОРАМИ

Проблемы

Расследование преступлений в Интернете очень часто требует тесного сотрудничества между частными компаниями (такими, как Интернет-провайдеры) и правоохранительными органами. Такое сотрудничество охватывает следующие аспекты:

- Выявление подозреваемых на основе IP-адреса или реквизитов банковского счета
- Сообщение информации о подписчике
- Идентификация и доступ к сохраненному незаконному содержанию.

Для частного сектора сотрудничество с правоохранительными органами может привести к конфликтам в тех случаях, когда не создана юридическая основа для такого сотрудничества. Поэтому партнерские связи между государственным и частным секторами имеют особое значение в связи с двумя аспектами:

- Улучшение сотрудничества в существующих юридических рамках

- Развитие принципов для осуществления или совершенствования процедур партнерских связей между государственным и частным секторами

Партнерские связи между государственным и частным секторами при проведении расследования в Интернете не могут расширяться безгранично. Такие ограничения связаны, например, с тем, что ключевые аспекты расследования уголовных дел должны - по крайней мере в большинстве стран - оставаться под полным контролем компетентных правоохранительных органов.

Обмен передовой практикой

Важность партнерских связей между государственными и частными секторами была и остается определяющим фактором для осуществления ряда инициатив. С учетом того, что многие всемирные партнеры в Интернет-бизнесе имеют свои штаб-квартиры в США, эти компании играют важную роль. Передовая практика, представленная во время Конференции, включает:

- Партнерство между Советом Европы и Микрософтом по поддержке проекта по киберпреступности и тем самым продвижение Конвенции по киберпреступности во всем мире
- Систему отслеживания эксплуатации детей, разработанную Микрософтом, в партнерстве с канадскими правоохранительными органами, которая в настоящее время применяется в ряде стран
- Лондонский план действий, который направлен на международное сотрудничество правоохранительных органов в борьбе со спамом
- Рабочую группу по борьбе с фишингом (APWG), которая является всемирной ассоциацией всех отраслей промышленности и правоохранительных органов по борьбе с мошенничеством и кражей личности, связанных с фишингом, фармингом и спуфингом в электронной почте разного типа. В настоящее время в группу входит несколько тысяч членов, агентств и компаний по всему миру
- Подгруппу Большой восьмерки по преступности в сфере высоких технологий, которая поощряет страны присоединяться к сети контактных пунктов в сфере высоких технологий 24/7 и использовать преимущества работы подгруппы на основе сотрудничества между промышленными компаниями и правоохранительными органами, защиты жизненно важной информационной инфраструктуры, сохранения данных и других вопросов. Документы и передовая практика в этих областях размещены на сайте www.coe.int/economiccrime
- Сотрудничество между правоохранительными органами и частным сектором в Сербии

Перспективы

- Следует и далее развивать и расширять партнерские связи между государственным и частным секторами
- При этом следует продолжать проводить анализ ограничений в области партнерства между государственным и частным секторами
- Следует выявлять региональных участников и включать их в сети наряду со всемирными участниками
- На основе передовой практики требуется разрабатывать руководящие принципы или правила для партнерства между государственным и частным секторами.

7 РОЛЬ ИНТЕРНЕТ-ПРОВАЙДЕРОВ

Проблема

Интернет-провайдеры играют важную роль для будущего успеха сети. Без услуг, предоставляемых провайдером доступа, цель достижения того, чтобы как можно больше людей получили доступ к источникам Интернета, не может быть достигнута. Без возможности хранения данных, которые предоставляются хостинг-провайдерами, часто без дополнительной оплаты на уровне баз данных - пользователи Интернета в развивающихся странах потеряют важный инструмент обмена своими данными с другими пользователями. Для защиты этих интересов пользователей и для оказания им поддержки требуется, чтобы законодательство принимало во внимание защиту работы провайдеров доступа. Это включает обсуждение такого вопроса, как ограничение уголовной ответственности за правонарушения, совершаемые их клиентами.

Помимо обеспечения безопасности работы в Интернете, Интернет-провайдер играет важнейшую роль в расследованиях дел, связанных с Интернетом. Они могут оказывать особую помощь полиции и правоохранительным органам для того, чтобы:

- блокировать веб-сайты;
- выявлять и удалять незаконное содержание;
- выявлять правонарушителей;
- оказывать содействие в установке инструментов расследования;
- собирать данные (хранение данных/удержание данных);
- предупреждать преступления (нарушение авторских прав, спам).

Обмен передовой практикой

- Вновь началось обсуждение об уточнении обязанностей и прав Интернет-провайдера
- Основные принципы содержатся в директиве ЕС об электронной торговле
- Конвенция о киберпреступности в отношении обязательств Интернет-провайдеров оказывать содействие правоохранительным органам

Перспективы

- Следует продолжать открытое обсуждение о роли Интернет-провайдеров и связанных с этим правовых рамок. Необходимо документально зафиксировать передовую практику с целью разработки общих стандартов или руководящих принципов.

Кратко:

1. Улучшать анализ киберпреступности, содействовать сообщениям со стороны пострадавших, укреплять информированность и поощрять меры по предупреждению и защите отдельных лиц и общественности, а также пользователей в частном секторе и в важнейших инфраструктурах
2. Выполнять Конвенцию о киберпреступности и Протокол к ней и предоставлять для этого всю необходимую поддержку
3. Обмениваться информацией о законодательстве в области киберпреступности и анализировать его эффективность
4. Принимать меры по дальнейшему укреплению функционирования контактных пунктов 24/7
5. Продолжать действовать на прагматичной основе в отношении сотрудничества между разными инициативами и организациями; создавать сети и использовать существующие возможности
6. Осуществлять шаги по дальнейшему укреплению партнерских связей между государственным и частным сектором
7. В отношении роли Интернет-провайдеров: документально фиксировать передовую практику и рассмотреть возможность разработки общих руководящих принципов, принимая во внимание тот факт, что требуется тщательно сохранять равновесие между обеспечением безопасности и правом на частную жизнь

В общем: сотрудничать.

Страсбург, 12 июня 2007 года