



Экономический и Социальный Совет

Distr.: General

20 Desembre 2009

Original: Russian

Комиссия по предупреждению преступности и уголовному правосудию

Доклад о работе Модели*
(2 – 4 декабря 2009 года)

Содержание

Глава I
Правила процедуры Модели Комиссии по предупреждению преступности и уголовному правосудиюс. 1
Глава II
Повестка дня Модели Комиссии по предупреждению преступности и уголовному правосудиюс. 8
Глава III
Доклад «Меры по борьбе с преступлениями, связанными с использованием компьютеров»с. 9
Глава IV
Участники и организация работы Модели Комиссии по предупреждению преступности и уголовному правосудиюс. 22
Глава V
Резолюция, принятая Моделью Комиссии по предупреждению преступности и уголовному правосудиюс. 25

* Доклад подготовлен по результатам первой Модели Комиссии по предупреждению преступности и уголовному правосудию, заседания которой проходили в Московском государственном институте международных отношений (Университете) Министерства иностранных дел Российской Федерации, г. Москва.

Глава I

Правила процедуры Модели Комиссии по предупреждению преступности и уголовному правосудию.

Часть I. Общие положения.

Правило 1. Правила процедуры

1. Настоящие Правила процедуры (далее – «Правила процедуры», «Правила») Комиссии по предупреждению преступности и уголовному правосудию (далее – Комиссии) утверждаются до начала Модели ООН. Правила процедуры могут быть изменены только Секретариатом Модели ООН.
2. Право толкования любых положений Правил процедуры принадлежит Председателю Комиссии.

Правило 2. Язык

Русский язык является рабочим языком Комиссии.

Правило 3. Полномочия

1. Полномочия делегатов удостоверяются до начала конференции Секретариатом Модели ООН во время регистрации Представителей.
2. Представители не должны злоупотреблять настоящими Правилами.
3. Во время выступления Представитель не может выступать от себя лично.

Правило 4. Делегаты

1. Каждая страна может быть представлена только одним делегатом.
2. Делегаты имеют право выступать и голосовать по всем вопросам.

Правило 5. Бюро.

1. Бюро Комиссии состоит из Председателя, Заместителя Председателя, Докладчика и двух секретарей.
2. Докладчик готовит доклад по вопросам повестки дня и участвует в заседаниях Комиссии. Докладчик дает заключение о соответствии всех подаваемых проектов резолюции и поправок к проекту резолюции требованиям к оформлению резолюции, нормам международного права и принятым решениям ООН. Заключение Докладчика не может быть опротестовано. Председатель может в любое время обратиться к Докладчику за разъяснением по фактическим или юридическим вопросам. Любой из делегатов в ходе прений может с разрешения Председателя запросить разъяснений Докладчика по таким вопросам, после чего слово может быть предоставлено Докладчику по решению Председателя.
3. Секретари выполняют свою работу под непосредственным руководством Председателя. Они принимают, печатают и распространяют документы, доклады и резолюции Комиссии, ведут подсчет голосов при голосовании, а также выполняют другую работу для обеспечения деятельности Комиссии по поручению Председателя.

Правило 6. Председатель

1. Председатель ведет заседания, руководствуясь правилами процедуры, и стремится обеспечить эффективную работу органа.
2. Председатель:

-
- следит за соблюдением настоящих Правил;
 - проводит переключку с целью установления наличия кворума в начале каждого заседания, а также в любое другое время, в случае, если возникнет необходимость;
 - открывает и закрывает каждое пленарное заседание сессии;
 - полностью осуществляет руководство ходом каждого заседания;
 - вносит предложения процедурного характера;
 - руководит прениями на пленарных заседаниях;
 - объявляет о начале срока для внесения проектов резолюций или поправок;
 - открывает и закрывает список ораторов;
 - предоставляет слово;
 - поддерживает порядок на заседании;
 - ставит вопросы на голосование;
 - объявляет решения.

3. Председатель имеет право не рассматривать вопросы и предложения, выдвигаемые Представителями, в случае, если это отдельно не оговорено в правилах процедуры Модели ООН.

4. Председатель выносит постановления по вопросам, которые Правилами процедуры оставлены на его усмотрение, а также по любым вопросам, относящимся к ведению заседания и не регламентированным данными правилами.

5. Постановления Председателя могут быть опротестованы. Такой протест должен быть поддержан хотя бы одной делегацией, помимо делегации, внесшей предложение, после чего он ставится на голосование. Постановление Председателя остается в силе, если оно не отменяется квалифицированным большинством в две трети присутствующих и участвующих в голосовании.

6. Председатель должен сохранять беспристрастность. Председатель должен воздерживаться от высказываний по существу обсуждаемых вопросов, за исключением случаев, когда такое обсуждение может нанести серьезный ущерб целям и принципам ООН. Председатель голосует лишь в случае, если голоса разделились поровну (за исключением вопросов по процедуре).

Правило 7. Повестка дня

Повестка дня утверждается до начала конференции и не может быть изменена.

Часть II. Ведение заседания.

Правило 8. Кворум.

1. Председатель может объявить заседание открытым и разрешить проведение прений, если в зале присутствуют одна треть делегаций Комиссии, зарегистрировавшихся на Модели.

2. Для принятия любого решения требуется присутствие простого большинства делегаций Комиссии.

3. В целях установления (присутствия) наличия кворума Председатель проводит переключку в алфавитном порядке. Делегаты, заявившие во время переключки

«присутствую и голосую», не могут воздерживаться от голосования по каким бы то ни было вопросам.

Правило 9. Регламент выступлений.

1. Комиссия может ограничить время, предоставляемое каждому оратору.
2. Соответствующее решение Комиссия принимает на основании процедурного предложения, с которым может выступить какой-либо Делегат или Председатель.
3. Решение об установлении регламента выступлений принимается простым большинством голосов.
4. Если прения были ограничены, и представитель превысил предоставленное ему время, Председатель немедленно призывает его к порядку.

Правило 10. Общие прения.

В начале каждой сессии Комиссии проводятся общие прения, в ходе которых каждый делегат может выступить с изложением позиции страны по обсуждаемому вопросу. Каждый делегат может выступать в общих прениях только один раз. Продолжительность выступления и количество вопросов оратору может быть ограничено соответствующими процедурными предложениями.

Правило 11. Список ораторов.

1. Во время заседания применяются правила формальных прений, если Комиссия не приняла другого решения. Председатель составляет список ораторов.
2. Представитель может быть добавлен в список ораторов, если он поднимает свою табличку.
3. В случае если невозможно определить, кто из Представителей поднял табличку первым, Председатель сам определяет очередность выступлений, руководствуясь принципом равенства и стремлением улучшить работу органа.

Правило 12. Выступления.

1. Представитель не может выступать, если Председатель не предоставил ему слово.
2. Время выступлений может быть ограничено (см. Правило 11).
3. В случае если Представитель выступает без разрешения Председателя, превышает лимит времени, если его заявления не соответствуют обсуждаемой теме или являются агрессивными, либо Представитель нарушает Правила Процедуры иным образом, Председатель призывает Представителя к порядку. Полномочия Представителя могут быть отозваны руководством Модели ООН в случае грубых и неоднократных нарушений правил процедуры, неуважительного отношения к Председателю, другим Представителям, Модели ООН или к Организации Объединённых Наций.
4. Диалог между Представителями во время формальных дебатов недопустим.
5. После выступления Представителя другие Представители имеют право задавать ему вопросы, время которых может быть ограничено (см. п. 11 Правил). Время, в течение которого задаются вопросы и даются ответы на них, не засчитывается в общее время выступления Представителя. Оратор имеет право не отвечать на вопросы.

Правило 13. Вопрос личной привилегии.

1. В любой момент заседания (за исключением голосования) каждый Представитель может выступить по вопросу личной привилегии только в том случае, если Представитель испытывает какое-либо личное неудобство. После того как

Председатель предоставит ему слово, Представитель должен встать и объяснить свою жалобу.

2. При выступлении по вопросу личной привилегии Представитель не может высказываться по существу обсуждаемой темы.

Правило 14. Вопрос по ведению заседания.

В любой момент заседания каждый Представитель может поднять вопрос по порядку ведения заседания, который немедленно решается Председателем в соответствии с настоящими Правилами. Представитель, выступающий по порядку ведения заседания, не может говорить по существу обсуждаемого вопроса.

Правило 15. Предложение перейти к неформальным дебатам под председательством.

1. Неформальные дебаты под председательством используются для неформального продолжения обсуждения.

2. Любой Делегат либо Председатель в любой момент заседания (но не во время выступления, не во время проведения голосования) может внести предложение о переходе к неформальным дебатам. Когда Председатель предоставит Делегату слово, он должен встать, объяснить цель предлагаемых неформальных дебатов и указать, на какой период предлагается объявить неформальные дебаты.

3. Данное предложение требует поддержки хотя бы ещё одной делегации и сразу ставится на голосование. Для принятия решения о переходе к неформальным дебатам необходимо простое большинство голосов Делегатов Комиссии.

Правило 16. Предложение перейти к неформальным дебатам.

1. Неформальные дебаты прерывают ход заседания. Это время используется для проведения переговоров.

2. Каждый Делегат либо Председатель в любой момент заседания (но не во время выступления и не во время проведения голосования) может внести предложение о переходе к неформальным дебатам без председательствования. Когда Председатель предоставит Представителю слово, он должен встать, объяснить цель предлагаемых неформальных дебатов и указать на какой период объявляются неформальные дебаты.

3. Данное предложение требует поддержки хотя бы ещё одной делегации, не обсуждается и сразу ставится на голосование. Для принятия решения о переходе к неформальным дебатам без председательствования необходимо простое большинство голосов делегатов Комиссии.

Правило 17. Предложение о переходе к формальным дебатам.

1. Каждый Делегат либо Председатель в любой момент заседания до окончания установленного срока неформальных дебатов (но не во время выступления) может внести предложение о переходе к формальным дебатам. Когда Председатель предоставит Представителю слово, он должен встать и объяснить цель предлагаемых формальных дебатов.

2. Данное предложение требует поддержки хотя бы ещё одной делегации, не обсуждается и сразу ставится на голосование. Для принятия решения о переходе к формальным дебатам необходимо большинство голосов делегатов Комиссии.

Правило 18. Предложение о прекращении прений.

1. Прекращение прений означает окончание обсуждения и переход к голосованию.

2. Каждый Делегат в любой момент заседания (но не во время выступления) может внести предложение о прекращении прений. Данное предложение требует поддержки хотя бы ещё одной делегации.

3. Предложение о прекращении прений обсуждается, при этом действуют правила формальных дебатов. Обсуждение не может длиться дольше 5 минут. Для принятия решения о прекращении прений требуется простое большинство голосов Делегатов.

Правило 19. Последовательность обсуждения вопросов и предложений.

Следующие процедурные предложения ставятся на голосование в приоритетном порядке:

- о перерыве в работе заседания;
- о закрытии заседания;
- о перерыве в прениях по обсуждаемому вопросу;
- о прекращении прений по обсуждаемому вопросу.

Часть III. Резолюция

Правило 20. Проект резолюции.

1. После завершения общих прений Председатель объявляет начало срока подачи проектов резолюций. Срок подачи резолюций может быть ограничен в соответствии с настоящими Правилами (см. Правило 11).

2. Проект резолюции считается поданным, если по нему получено заключение Докладчика о том, что данный проект соответствует требованиям к оформлению проектов резолюции, не противоречит нормам международного права и ранее принятым резолюциям, и он зарегистрирован Председателем.

3. Поданные проекты резолюции регистрируются Председателем Комиссии, им присваивается порядковый номер, далее они передаются Секретарям для размножения и распространения среди Делегатов, после чего возможно их формальное обсуждение. Проекты резолюции обсуждаются в том порядке, в каком они были зарегистрированы Председателем, если Комиссии не решит иначе.

4. На обсуждении может находиться больше, чем один проект резолюции.

Правило 21. Принятие рабочего проекта резолюции.

Принятие рабочего проекта резолюции (из числа представленных проектов резолюции) требует простого большинства голосов делегатов Комиссии. Проекты резолюций обсуждаются и выносятся на голосование в порядке, в котором они были представлены Председателю.

Комиссия рассматривает все поступившие проекты резолюции в порядке их регистрации Председателем. Комиссия может принять один или несколько проектов резолюции в качестве рабочих; в последнем случае обсуждение проектов происходит в порядке их регистрации Председателем.

Часть IV. Поправки.

Правило 22. Поправки.

1. Поправкой считается предложение, которое лишь добавляет что-либо к рабочему проекту резолюции, исключает что-либо из него или изменяет часть его. Поправки представляются в письменной форме докладчику для оценки их соответствия международному праву и предыдущим решениям ООН и последующей передачи Председателю Комиссии. Каждая поправка должна быть написана или напечатана на

отдельном листе бумаги, и содержать точное указание, к какой части рабочего проекта резолюции относится поправка, и какая страна ее предлагает.

2. Поправка не должна противоречить смыслу и целям рабочего проекта резолюции.
3. Грамматические, орфографические, синтаксические и стилистические ошибки в Рабочем проекте резолюции, не влияющие на смысл его текста, исправляются Секретариатом без голосования.

Правило 23. Поправки к поправке (поправки второго порядка).

1. Поправкой к поправке считается предложение, которое только добавляет что-либо к поправке, исключает что-либо из нее или изменяет ее часть.
2. Поправка к поправке делается в устной форме во время обсуждения основной поправки. Предлагающий ее Делегат должен четко сформулировать свое предложение, которое сразу ставится на голосование. Не допускается подача поправки к поправке после голосования по основной поправке.
3. При подаче нескольких поправок второго порядка к одной поправке такие поправки второго порядка обсуждаются в порядке их внесения.
4. После голосования по поправке к поправке Комиссии возвращается к обсуждению поправки в целом. Поправки третьего порядка и выше не допускаются.

Часть V. Голосование.

Правило 24. Голосование.

1. В случае если закончился список ораторов или было принято предложение о прекращении прений, резолюция, поправка или проект резолюции выносятся на голосование.
2. Каждый Делегат обладает 1 голосом: «за», «против» или «воздерживаюсь». Делегаты не могут воздерживаться при голосовании по процедурным вопросам. Делегаты, заявившие, что они присутствуют и голосуют, не могут воздерживаться при голосовании по любым вопросам.
3. Представители не могут переговариваться во время голосования. Ничто не может прерывать ход голосования (в том числе вопрос личной привилегии).
4. Во время голосования запрещается передвижение Делегатов в зале заседаний, вход в зал и выход из него.

Правило 25. Необходимое большинство.

1. Процедурные вопросы должны решаться простым большинством голосов. В случае если голоса разделяются поровну, решение считается не принятым.
2. Решения по принятию поправок, рабочего проекта резолюции и собственно резолюции принимаются простым большинством голосов.

Правило 26. Способ голосования.

1. Если Комиссии не примет другого решения, голосование проводится поднятием табличек.
2. В случае голосования по особо важному вопросу один из Делегатов может внести предложение о поименном голосовании. Такое предложение без обсуждения сразу ставится на голосование и принимается в том случае, если его поддержит простое большинство присутствующих и участвующих в голосовании Делегатов. При поименном голосовании вызывается каждый член Организации, его представитель отвечает “за”, “против” или “воздерживаюсь”. Поименное голосование проводится в русском алфавитном порядке.

Правило 27. Голосование по поправкам.

1. Поправки обсуждаются в соответствии с тем, к какому Правилу рабочего проекта резолюции они относятся непосредственно перед рассмотрением этого Правилу.
2. Если вносятся две и более поправки к одному Правилу, их рассмотрение начинается с поправки наиболее удаленной по смыслу от содержания рассматриваемого Правилу резолюции, затем рассматривается следующая поправка наиболее отдаленная по смыслу от содержания данного Правилу и так до завершения рассмотрения всех поправок к данному Правилу резолюции. Если необходимым следствием принятия одной поправки является отклонение другой поправки, последняя поправка не ставится на голосование.
3. После обсуждения всех поправок производится голосование по измененному таким образом рабочему проекту резолюции.
4. До проведения голосования Комиссии определяет количество ораторов выступающих за и против данной поправки и предоставляет им определенное время для выступления.

Глава II

Повестка дня Модели Комиссии по предупреждению преступности и уголовному правосудию.

02.12.2009 – среда – Зал № 2 МГИМО(У) МИД России.

09:30-10:00 - Регистрация участников.

10:00-10:30 - Торжественная церемония открытия (выступление Координатора Московской Международной Модели ООН Г.М. Ковриженко, профессора кафедры уголовного права, уголовного процесса и криминалистики А.Г. Волеводза, Генерального секретаря Московской Международной Модели ООН 2010 года В.Х. Аносовой).

10:30-11:00 - Тренинг по Правилам процедуры.

11:00-11.30 – Выступление преподавателя кафедры уголовного права, уголовного процесса и криминалистики В.В. Дубровина по вопросу повестки дня.

11:30-14:00 - Заседания в органе.

14:00-14.30 – Обед.

14:30-16:00 - Заседания в органе.

03.12.2009 – четверг – Аудитория № 4154 МГИМО(У) МИД России.

10:00-13:00 - Заседания в органе.

13:00-14:00 – Обед.

14:00-16:00 - Заседания в органе.

04.12.2009 – пятница – Зал №5 МГИМО(У) МИД России.

10:00-14:00 –Заседания в органе.

14:00-15:00 – Обед.

15:00-16:00 - Торжественная церемония закрытия (отчет Председателя о работе Комиссии, выступление преподавателя кафедры уголовного права, уголовного процесса и криминалистики В.В. Дубровина с оценкой работы Модели, вручение

заведующим кафедры уголовного права, уголовного процесса и криминалистики А.С. Подшибякиным сертификатов участникам Модели, выступление Координатора Московской Международной Модели ООН Г.М. Ковриженко).

Глава III

ДОКЛАД: Меры по борьбе с преступлениями, связанными с использованием компьютеров.

Подготовлен: Стахеевой Юлией Александровной, студенткой 4 курса Международно-правового факультета МГИМО(У) МИД России (г. Москва)

Содержание доклада:

Введение

Статистика

Понятие киберпреступности и классификация киберпреступлений

Попытки законодательного урегулирования кибербезопасности

Методы борьбы с киберпреступностью

Выводы

ВВЕДЕНИЕ

В наши дни большинство людей значительную часть своего времени проводят в Интернете. Этот виртуальный мир во многом отражает мир реальный: преступность, являющаяся, к сожалению, неотъемлемой частью социума, существует и в виртуальном мире.

Растущий обмен информационными данными в Интернете и электронные платежи – это именно тот лакомый кусок, который более всего привлекает злоумышленников.

Киберпреступность стала настоящим бизнесом и развивается так же, как и любой другой бизнес. Важными для нее являются прибыльность, управление рисками, освоение новых рынков.

Почему же она получила такое большое развитие в современном мире?

Во-первых, киберпреступность невероятно прибыльна! Огромные суммы денег оказываются в карманах преступников в результате отдельных крупных афер, не говоря уже о небольших суммах, которые идут просто потоком. Например, только в 2007 году практически каждый месяц совершалось одно серьезное преступление с использованием современной вычислительной и электронной техники:

Январь 2007.	Российские хакеры с помощью своих шведских «коллег» похитили 800 000 ЕВРО из шведского банка Nordea
Февраль 2007	Бразильская полиция арестовала 41 хакера за использование троянской программы для кражи банковской информации, которая позволила им заработать 4,74 миллиона \$
Февраль 2007	В Турции арестованы 17 членов банды интернет-мошенников, которым удалось похитить около 500 000 \$
Февраль 2007	Арестован Ли Чжун, создатель вируса «Панда» (Panda burning Incense), нацеленного на кражу паролей к онлайн-играм и учетным записям систем интернет-пейджинга. Предполагается, что на продаже своей

	вредоносной программы он заработал около 13 000 \$
Март 2007	Пять граждан восточно-европейских государств посажены в тюрьму в Великобритании за мошенничество с кредитными картами, их добыча составила порядка 1,7 миллионов фунтов стерлингов
Июнь 2007	В Италии арестованы 150 киберпреступников, которые забрасывали итальянских пользователей мошенническими сообщениями. Их доход составил почти 1,25 миллионов евро
Июль 2007	По неподтвержденным данным российские киберворы, используя троянскую программу, похитили 500 000 \$ у турецких банков
Август 2007	Украинец Максим Ястремский, известный также как Maksik, задержан в Турции за кибермошенничество с использованием электронных систем и незаконное присвоение десятков миллионов \$
Сентябрь 2007	Грегори Копилофф (Gregory Kopiloff) обвинен властями США в краже персональных данных с помощью файлообменных сетей Limewire и Soulseek. Полученную информацию он использовал для реализации мошеннических схем и выручил на этом тысячи долларов
Октябрь 2007	В США арестован Грег Кинг (Greg King) за участие в организации февральской DDoS-атаки на сайт Castle Cops. Его приговорили к десяти годам тюремного заключения и штрафу 250 000 \$
Ноябрь 2007	ФБР арестовало восемь человек в ходе второй части операции Operation Bot Roast по борьбе с ботсетями. По результатам операции была названа сумма экономического ущерба, составившая более 20 млн. \$, и выявлено более миллиона компьютеров-жертв
Декабрь 2007	Киберпреступники взломали компьютеры департамента энергетики Национальной лаборатории Оак Риджа (ORNL), Теннесси, США. По имеющимся данным атаке подверглись также Национальная лаборатория в Лос Аламосе и Национальная лаборатория Лоуренса в Ливерморе, Калифорния. Были украдены более 12 000 номеров карт социального страхования и дат рождения посетителей ONRL за период с 1999 до 2004. Этот инцидент – из ряда проблем национальной безопасности, поскольку демонстрирует незащищенность отдельной личности в случае кражи идентификационных данных и финансового мошенничества

Во-вторых, успех дела не связан с большим риском. В виртуальном мире преступники не могут видеть своих жертв, будь то отдельные люди или целые организации, которые они выбрали для атаки. Грабить тех, кого ты не видишь, гораздо легче.

В-третьих, уровень технической подготовки, необходимый для того чтобы запустить киберкриминальный бизнес, становится все ниже. Существует масса анонимных интернет-ресурсов, предлагающих все что угодно: от эксплуатации уязвимостей до троянских программ. Сейчас вирусы могут создавать и управлять ими студенты и даже школьники.

В-четвертых, через Интернет сейчас становятся доступны все более новые сервисы. И миллионы желающих этими сервисами пользоваться способствуют успеху киберпреступности. В пример можно привести следующие области предоставления услуг, наиболее уязвимые для атак:

- Интернет-деньги и интернет-банки.

- Удаленные хранилища данных и приложений. Информацию и приложения все чаще размещают на удаленных внешних серверах, что позволяет преступникам взламывать трафик и получать доступ к финансовой, конфиденциальной и личной информации.
- Онлайн-игры. Преступления в этой области – это кража паролей и виртуальной собственности для последующей их продажи и получения хорошей прибыли.
- Биржевые агентства онлайн. Удобный и быстрый способ реагировать на колебания рынка ценных бумаг. Он является весьма привлекательной целью для преступников, потому что любая биржевая информация всегда пользуется повышенным спросом.
- Web 2.0. Социальные сети, блоги, форумы, wiki-ресурсы, MySpace, YouTube, Twitter – все эти легкие в загрузке и публикации технологии обмена информацией делают его участников уязвимыми для заражений вредоносными программами.

В-четвертых, во многих случаях правоохранные органы отстают от преступников, испытывая недостаток технологий и квалифицированного персонала для отражения новой и быстро растущей угрозы.

СТАТИСТИКА

Лаборатория PandaLabs проанализировала безопасность в Интернете за июль-сентябрь 2009 года и отметила, что активность киберпреступников бьет рекорды: в третьей четверти текущего года было выявлено около пяти млн новых видов вредоносного ПО. Ежедневно специалисты имеют дело примерно с 50 тыс. новых троянов, шпионских и рекламных модулей, вирусов, руткитов и т. п. Для сравнения: несколько месяцев назад сотрудники PandaLabs ежедневно фиксировали менее 40 тыс. ранее неизвестных модификаций вредоносного ПО.



Диаграмма 1: Распределение вредоносных программ по типам (PandaLabs)

По сравнению с предыдущим кварталом количество зараженных компьютеров выросло на 15%. Более чем в 37% случаев заражение вызывали трояны, причиной 18,7% инфекций стали рекламные коды, что, в свою очередь, оказалось вызвано быстрым распространением фальшивых антивирусов.

В третьем квартале в общей массе новых вредоносных кодов, обнаруженных PandaLabs, доминировали трояны, доля которых составила около 71%. Доля рекламных программ сократилась с 16,4% во втором квартале до 13,1% в третьем. Количество шпионских модулей, напротив, незначительно увеличилось, достигнув 9,2%.

Эксперты подчеркивают, что традиционные вирусы и черви практически исчезли: они насчитывают всего 2% от общего числа вредоносных программ. Вместе с тем наблюдается экспансия нежелательных кодов через спам, социальные сети и поисковые движки, которые ведут на фальшивые веб-страницы.

Большой проблемой является отсутствие точных статистических данных об этих правонарушениях. Сообщение о преступлениях производится на добровольной основе. Это означает, что количество преступлений, о которых сообщается, намного ниже, чем фактическое их количество. О неизвестном количестве преступлений не сообщается еще и из-за того, что о большинстве преступлений, которые зарегистрированы полицией, не сообщается в агентства, собирающие статистику.

ПОНЯТИЕ КИБЕРПРЕСТУПНОСТИ И КЛАССИФИКАЦИЯ КИБЕРПРЕСТУПЛЕНИЙ

Проблема киберпреступности волнует как отдельные государства, так и международные организации, и все мировое сообщество в целом.

Одной из основных трудностей в борьбе с киберпреступностью является терминологическая неясность. Непонятно, что же нужно относить к киберпреступлениям.

На X Конгрессе ООН по предупреждению преступности и обращению с правонарушителями на симпозиуме по проблемам преступлений, связанных с компьютерами и компьютерными сетями, киберпреступления были подразделены на следующие две категории:

- а. Киберпреступление в узком смысле (компьютерное преступление): любое противоправное деяние, совершенное посредством электронных операций, целью которого является безопасность компьютерных систем и обрабатываемых ими данных.
- б. Киберпреступление в широком смысле (как преступление, связанное с компьютерами): любое противоправное деяние, совершенное посредством или связанное с компьютерами, компьютерными системами или сетями, включая незаконное владение [и] предложение или распространение информации посредством компьютерных систем или сетей.

Во многих случаях преступления, которые мы можем согласно нашему общему определению назвать “киберпреступлениями” - в действительности уже существуют, за исключением того, что при их совершении так или иначе используется компьютерная сеть. Таким образом, человек мог использовать Интернет для построения финансовых пирамид, рассылки “писем счастья”, привлечения клиентов в притоны, сбора ставок для нелегальных азартных игр, скачивания детской порнографии. Все эти деяния уже являются незаконными во многих юрисдикциях и могли бы быть совершены без использования компьютерной сети. “Кибер” аспект не является необходимым элементом преступления, а служит лишь средством совершения преступления. Компьютерные сети предоставляют преступникам новые способы совершения “старых” преступлений.

Существующие законы, запрещающие подобные действия, могут применяться к лицам, совершившим эти деяния с помощью компьютеров и сетей, точно так же как к тем, кто совершил их без использования новых технологий.

В других случаях преступление является уникальным и обязано своим существованием появлению сети Интернет. В качестве примера можно привести незаконный доступ. Он может быть уподоблен незаконному проникновению в дом или офисное здание, но признаки незаконного компьютерного доступа отличаются от признаков физического взлома. В определении, данном в законах, взлом и проникновение обычно требуют физического входа на территорию помещения, признака, который не представлен в преступлении, произошедшем в киберпространстве. Таким образом, новые законы должны учитывать эту специфику.

Кроме того, киберпреступность является относительно новой формой преступной деятельности, для которой не существует государственных границ: в киберпространстве преступники способны в считанные секунды сменить свое местонахождение из одной страны в другую, независимо от своего фактического расположения. Соответственно, для того чтобы эффективно бороться с киберпреступностью, необходимо далее укреплять международное сотрудничество. Исключительно важно также предоставить тем развивающимся странам, в которых отсутствуют необходимые для борьбы с киберпреступностью возможности и специальные знания, техническую помощь и учебно-методические пособия, поскольку это позволит им не только обмениваться знаниями и информацией, для того чтобы надлежащим образом выявлять и расследовать киберпреступления и осуществлять уголовное преследование за их совершение, но также преодолеть углубляющуюся "цифровую пропасть" между развивающимися и развитыми странами в области информационно-коммуникационных технологий¹.

В ходе различных исследований была разработана классификация категорий киберпреступлений.

Она основывается на разделении их на: 1) насильственные или иные потенциально опасные; и 2) ненасильственные преступления.

Насильственные или иные потенциально опасные

Насильственные и иные потенциально опасные преступления имеют наибольшую опасность по очевидным причинам – они представляют собой физическую опасность человеку или группе лиц. Эти преступления включают в себя:

- Кибертерроризм
- Угроза физической расправы
- Киберпреследование
- Детская порнография.

Появление интернета привело к увеличению разнообразия, объема и доступности сексуально оскорбительных изображений, в том числе детской порнографии, создав среду для их распространения и обеспечив растущий рынок для их потребления. Существует устойчивое ядро веб-сайтов, посвященных сексуальному насилию над детьми, большая часть которых являются коммерческими и приносят огромные

¹ См. обсуждения, состоявшиеся в последние годы в рамках Форума по вопросам управления использованием интернета, являющегося платформой для проведения политического диалога с участием многих заинтересованных сторон по проблемам интернета, учрежденной Генеральным секретарем Организации Объединенных Наций в соответствии с мандатом от Всемирной встречи на высшем уровне по вопросам информационного общества, в особенности обсуждения по двум тематическим областям, касающимся "безопасности" и "доступа" (<http://www.intgovforum.org/cms/index.php/home>).

доходы организованным преступным группам. Это, в свою очередь, создает проблемы для правоохранительных органов, уделяющих все больше внимания и средств борьбе с онлайн-сексуальными преступлениями. Расследования такого рода в большинстве случаев сложны и отнимают много времени, потому что их часто приходится координировать между несколькими юрисдикциями, а преступные сети, против которых они направлены, используют различные степени защиты. Согласно оценкам, с 2005 года в мире было зарегистрировано примерно 3 тыс. веб-сайтов, связанных с сексуальными преступлениями. Для того чтобы глобальные партнерства могли положить конец этим преступлениям и расследовать их, правительствам, интернет-индустрии, полиции, телефонным "горячим линиям", неправительственным организациям, благотворительным учреждениям, оказывающим помощь детям, педагогам, психологам и следователям по финансовым делам необходимо объединить усилия с целью переломить ситуацию и свести к минимуму непрекращающуюся сексуальную эксплуатацию детей с помощью технологий. Наряду с этим такая преступная деятельность подчеркивает значение содействия налаживанию максимально эффективного сотрудничества между правоохранительными органами и поставщиками услуг интернета в борьбе с киберпреступностью².

Еще одной областью, в которой может потребоваться такое сотрудничество, являются социальные сети (MySpace, Facebook), которые благодаря быстрому развитию интернет-технологий приобретают все большую популярность в качестве одного из средств социального общения. Эта революция в области социального взаимодействия сопровождается разглашением сведений частного характера, которые могут быть неправомерно использованы преступниками и, следовательно, могут способствовать возникновению новых форм преступности, против которых необходимо будет вести борьбу.

Неправомерное использование интернета в террористических целях является серьезной угрозой, и необходимо приложить дополнительные усилия, для того чтобы добиться более глубокого понимания этой проблемы.

Ненасильственные киберпреступления.

Большинство киберпреступлений совершаются без применения насилия, это следствие того, что одна из основных характеристик виртуального мира – способность взаимодействия без физического контакта. Кажущаяся анонимность и "нереальность" виртуального взаимодействия – элементы, делающие киберпространство привлекательным местом для совершения преступлений.

Ненасильственные киберпреступления могут быть подразделены на следующие категории:

- Противоправное нарушение владения в киберпространстве;
- Киберворовство;
- Кибермошенничество;
- Разрушение

² См. заказанное Советом Европы исследование на тему сотрудничества между правоохранительными органами и поставщиками услуг интернета в борьбе с киберпреступностью: движение к общим руководящим принципам (июнь 2008 года) (http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/ Documents/Reports-Presentations/567_prov-d-wgSTUDY_25June2008.pdf), а также принятые 2 апреля 2008 года Руководящие принципы сотрудничества между правоохранительными органами и поставщиками услуг интернета в борьбе с киберпреступностью (http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf).

-
- Другие киберпреступления, например:
 - Реклама услуг проституции в сети Интернет
 - Незаконный оборот наркотиков с использованием сети Интернет
 - Азартные игры в Интернете
 - Отмывание денег с помощью электронного перемещения
 - Киберконтрабанда, или передача нелегальных товаров, например, шифровальных технологий, запрещенных в некоторых государствах, по сети Интернет.

Безусловно, как и все прочие виды противоправных действий, любые киберпреступления несут в себе немалую угрозу для людей, причем степень этой угрозы, на наш взгляд, не до конца еще осознана и оценена в обществе. Но даже тот незначительный опыт, который уже имеется в этой области, а тем более опыт наиболее развитых стран мира, со всей очевидностью свидетельствует о несомненной уязвимости любого государства. Тем более что киберпреступность не имеет государственных границ, и преступник в равной степени способен угрожать информационным системам, расположенным практически в любой точке земного шара. Такие преступления, как правило, выходят за рамки обычных и нередко представляют собой неразрешимые для действующего законодательства задачи. Особую озабоченность вызывает проблема расследования такого рода преступлений, следы которых компьютерными преступниками стираются или уничтожаются.

Другой особенностью киберпреступлений, еще более затрудняющей их обнаружение, является использование малогабаритных спутниковых систем связи, благодаря чему такие преступления могут совершаться на значительном расстоянии от объекта преступления буквально за доли секунды. При этом расследование таких преступлений может занимать недели, если не месяцы, давая возможность преступнику уничтожить следы преступления и избежать наказания.

ПОПЫТКИ ЗАКОНОДАТЕЛЬНОГО УРЕГУЛИРОВАНИЯ КИБЕРБЕЗОПАСНОСТИ

В России действует Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Важнейшим принципом правового регулирования отношений в сфере информации, информационных технологий и защиты информации является «обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации», то есть принятии правовых, организационных и технических мер, направленных на: обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа, реализацию права на доступ к информации.

На международном уровне несколько стран, включая США, направили силы на заключение по вопросам кибербезопасности взаимных соглашений о юридической помощи, экстрадиции, разграничении разведывательных полномочий, унификации законов таким образом, чтобы киберпреступники могли преследоваться в судебном порядке даже в том случае, когда преступление пересекает границы. Эти усилия направлены на решение таких проблем, как компьютерное мошенничество, детская порнография в Интернете, электронное пиратство, все формы незаконного доступа. Под действие этих соглашений попадают действия государства по развязыванию кибервойны и использованию компьютерных нападений в качестве военного оружия.

За последние несколько лет как Комиссия по наркотическим средствам, так и Комиссия по предупреждению преступности и уголовному правосудию, а также управляющие органы ЮНОДК вместе с одиннадцатым Конгрессом Организации Объединенных Наций по предупреждению преступности и уголовному правосудию в различных резолюциях, в частности в Бангкокской декларации одиннадцатого Конгресса от 2005 года, признали важный вклад Организации Объединенных Наций в проведение региональных и других международных форумов по борьбе с киберпреступностью. В Бангкокской декларации, в частности, вновь была подтверждена основополагающая важность осуществления действующих документов и дальнейшей разработки национальных мер по борьбе с киберпреступностью, а также приветствовались усилия, направленные на активизацию и расширение нынешнего сотрудничества в области предупреждения и расследования преступлений, связанных с использованием высоких технологий и компьютеров, а также уголовного преследования за такие преступления (резолюция 60/177 Генеральной Ассамблеи, Правила 15 и 16).

Существенную роль в координации усилий международного сообщества играет **Европейская Конвенция о киберпреступности 2001 года**³. Конвенция направлена на осуществление общей политики в вопросах уголовного права, целью которой является защита общества от киберпреступлений путем принятия соответствующих законодательных актов, а также путем расширения международного сотрудничества. Необходимость международного сотрудничества вызвана распространением цифровых технологий, конвергенцией и продолжающейся глобализацией компьютерных сетей.

На нормативном уровне Конвенция Совета Европы о киберпреступности создает правовую основу для сотрудничества в значительно более широком контексте, нежели круг государств – членов Совета Европы, поскольку она открыта для присоединения также и других государств. Однако, когда это уместно, для содействия международному сотрудничеству в данной области можно использовать также и **Конвенцию Организации Объединенных Наций против транснациональной организованной преступности**. Данная Конвенция обязывает государства-участники ввести ряд мер в целях укрепления взаимной правовой помощи, выдачи и других форм сотрудничества между судебными и правоохранительными органами в борьбе со всеми серьезными преступлениями, включая киберпреступления. Хотя Конвенция применяется лишь в тех случаях, когда имеет место деятельность организованной преступной группы, а такая группа квалифицируется как организованная преступная группа при условии, что одна из ее целей состоит в получении "финансовой или иной материальной выгоды", большая часть серьезных киберпреступлений подпадает под действие Конвенции. Во всяком случае, значение термина "финансовая или иная материальная выгода" является сравнительно широким и охватывает, например, совершаемые в онлайн-режиме преступления, связанные с противоправным использованием средств идентификации, когда похищенная или сфабрикованная идентификационная информация рассматривается в качестве незаконного товара, являющегося объектом купли, продажи или обмена, а также когда средства идентификации неправомерно используются для получения личной или коллективной выгоды, в том числе нефинансового характера, такой как возможность въезда в другую страну. Подход к "существу вопроса" как к своего рода незаконному товару, являющемуся объектом купли, продажи или обмена для организованных преступных групп, должен также применяться к использованию информационных технологий, в частности интернета, для совершения развратных действий в отношении детей и их сексуальной эксплуатации.

³ Council of Europe, *European Treaty Series*, No. 185.

МЕТОДЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

Для решения проблем киберпреступности необходимо применять широкие, комплексные подходы, выходящие за рамки уголовного и уголовно-процессуального законодательства, а также правоприменения.

Укрепление безопасности киберэкономики

В рамках такого подхода следует уделять внимание требованиям к безопасному функционированию киберэкономики, которые укрепляли бы доверие со стороны бизнеса и обеспечивали неприкосновенность частной жизни, равно как и стратегиям, направленным на продвижение и защиту нововведений, рост потенциала повышения благосостояния и возможностей информационных и компьютерных технологий, в том числе механизмам раннего предупреждения и реагирования в случае кибератак.

Создание глобальной культуры кибербезопасности

Помимо необходимости предотвращения преступлений, связанных с использованием компьютеров, и судебного преследования за их совершение появляется более глобальная задача – создание глобальной культуры кибербезопасности, в рамках которой учитывались бы потребности всех стран, включая развивающиеся, структуры информационных технологий в которых находятся в процессе становления и пока еще весьма уязвимы.

Активные действия ООН в сфере борьбы с киберпреступностью

Следует и далее развивать международное сотрудничество на всех уровнях. Система Организации Объединенных Наций, будучи универсальной по своему характеру, должна, при условии усовершенствования ее внутренних координационных механизмов, к чему призывает Генеральная Ассамблея, играть ведущую роль в межправительственных мероприятиях, направленных на обеспечение функционирования и защиту киберпространства, чтобы преступники или террористы не могли злоупотреблять им или воспользоваться им в своих целях. В частности, системе Организации Объединенных Наций следует сыграть важную роль в разработке глобальных подходов к борьбе с киберпреступностью и процедур международного сотрудничества, имея целью предупреждение и смягчение негативного влияния, которое оказывает киберпреступность на важнейшие элементы инфраструктуры, устойчивое развитие, защиту неприкосновенности частной жизни, электронную коммерцию, банковское дело и торговлю.

Обновление законодательства в отношении киберпреступности

Следует призвать все государства как можно быстрее обновить свое уголовное законодательство, чтобы учесть особый характер киберпреступности. Что касается традиционных видов преступлений, совершаемых с использованием новых технологий, то такое обновление может принять форму уточнения или изъятия норм, которые более не отвечают в полной мере сложившейся ситуации, например законов, которые не могут решать проблемы разрушения или хищения нематериальных активов, либо создания новых норм, касающихся новых видов преступлений, таких как несанкционированный доступ к компьютерам или компьютерным сетям.

Такое обновление должно касаться также процессуального законодательства (например, касающегося отслеживания сообщений) и законов, договоров или положений о взаимной правовой помощи (например, по вопросам оперативного обеспечения сохранности данных). Следует призывать государства руководствоваться при определении степени суровости вновь принимаемых законов положениями Европейской Конвенции о киберпреступности.

Специалисты называют пять основных направлений правового регулирования Интернет-отношений:

-
- защита личных данных и частной жизни в Сети;
 - регулирование электронной коммерции и иных сделок и обеспечение их безопасности;
 - защита интеллектуальной собственности;
 - борьба против противоправного содержания информации и противоправного поведения в Сети;
 - правовое регулирование электронных сообщений.

Повышение информационного образования лиц, участвующих в предотвращении, обнаружении киберпреступлений, борьбе с киберпреступностью

Сотрудники правоохранительных органов знают уголовный закон, а также основы сбора доказательств и вопросы предания правонарушителей правосудию. ИТ – персонал ориентируется в компьютерах и сетях, их работе, умеет отслеживать информацию в них. Каждый имеет свою “половинку ключа” к нанесению поражения киберпреступникам.

Поэтому для наиболее эффективной борьбы с киберпреступностью необходимо обучение каждого, кто участвует в предотвращении, обнаружении киберпреступлений, судебном преследовании тех, кто их совершил. Даже потенциальные киберпреступники, при наличии правильного образования, могут отклониться от преступного поведения.

Законодатели нуждаются в обучении основам информационных технологий – работе компьютеров, работе сетей. Эти образовательные программы должны быть направлены на целевую аудиторию – сотрудников законодательных и правоохранительных органов, а не просто быть повторением того, что дается при обучении ИТ – специалистов. Тем, кто расследует киберпреступления, не нужна детальная информация о том, как установить и формировать операционную систему. Но они должны знать то, как хакер может использовать “прорехи” в системе для неправомерного доступа в нее.

Обучение законодателей, чтобы они могли понять законы, которые они отдают свои голоса, отличается от обучения следователей, которым необходимо собрать цифровые доказательства. Последние должны пройти не только теоретическое, но и практическое обучение в работе с открытием данных и восстановлением, шифрованием и декодированием, чтением и интерпретацией контрольных файлов. Обвинители нуждаются в образовательных программах, направленных на понимание значения различных видов цифровых доказательств и порядок представления их в суде.

Использование влияния лидеров социальных групп для борьбы с киберпреступностью.

Один из способов сокращения количества киберпреступлений – использование влияния лидеров социальных групп. Если правонарушители не вызывают восхищения, наоборот, подвергаются осуждению, то менее вероятны случаи преступного поведения. Этот метод особенно эффективен в молодежной среде. Множество хакеров совершают взломы сети, чтобы произвести впечатление на друзей. Если бы молодым людям, интересующимся компьютерными технологиями, преподавали “кодекс компьютерной этики”, делая упор на то, что уважение к собственности других лиц в виртуальном мире столь же важно, как в мире физическом, хакеры вызывали бы не больше восхищения, чем “плохие парни”, занимающиеся грабежом или кражей автомобилей.

Использование технологий в борьбе с киберпреступностью.

Одним из лучших оружий против преступности в сфере высоких технологий являются сами технологии. Компьютерная промышленность прикладывает много усилий для создания техники и программного обеспечения, предназначенного для предотвращения и обнаружения вторжений в сети. Производители операционных систем встраивают в них все больше приспособлений для безопасности. В январе 2002 года Билл Гейтс объявил,

что для компании Microsoft важнейшим приоритетом впредь будет безопасность, для этого в компании были созданы специальные подразделения.

Сегодня на рынке присутствует множество доступных средств для препятствия вторжения в сеть и систему – от биометрических опознавательных устройств до программного обеспечения firewall. Контрольные и ревизионные программы позволяют ИТ – специалистам собирать детальную информацию для обнаружения подозрительных действий. Многие из них предусматривают уведомления об опасности, немедленно сообщаящие администраторам о происходящем нарушении.

Программы восстановления данных помогают сотрудникам правоохранительных органов осуществить сбор доказательств, несмотря на усилия преступников по их уничтожению. Полиция может – используя ордер на обыск – войти в защищенные системы преступников, используя их же методы доступа в системы.

Поиск новых способов защиты от киберпреступности

Невозможно предотвратить все киберпреступления или наверняка избежать вероятности стать их жертвой. Однако организации и частные лица могут заранее предпринять шаги для минимизации последствий киберпреступлений.

Например, The Austin Business Journal 28 апреля 2000 года сообщил, что компании начали заключать договоры о страховании ущерба, причиненного киберпреступлением. Поскольку киберпреступность растет, потенциальные жертвы ищут новые способы защиты от финансовых потерь.

Интерес представляют также научно-технологические достижения в области криминалистики. За последнее десятилетие важный технический прогресс в оснащении криминалистов и все более широкое использование научных методов в судопроизводстве внесли значительный вклад в борьбу с преступностью. Внедрение новых технологий ведет к постоянному повышению качества работ, выполняемых в местах совершения преступлений и в криминалистических лабораториях. Такие успехи способствовали повышению эффективности системы уголовного правосудия в раскрытии преступлений, осуждении преступников и оправдании невиновных.

Развитие международного сотрудничества в области борьбы с киберпреступностью

Следует уделить значительное внимание разработке, совершенствованию и развитию существующих ныне практических механизмов обмена информацией в международном масштабе, раннего предупреждения и реагирования, а также способов уменьшения ущерба в рамках борьбы с киберпреступностью, используя в этих целях возможности Интерпола, механизмов оперативного реагирования 24/7, разработанных "группой восьми", Конвенции по киберпреступлениям, Центров реагирования на компьютерные инциденты (CERT) и Форума центров компьютерной безопасности и реагирования на компьютерные инциденты (FIRST), которые пока распространяются лишь на отдельные, преимущественно развитые, страны. Эти механизмы следует сделать доступными на международном уровне, чтобы наладить обмен знаниями и информацией о путях и методах распознавания, защиты, недопущения и борьбы с новыми видами киберпреступлений и информировать общество об эффективных механизмах реагирования. Кроме того, особо следует позаботиться о том, чтобы эти практические механизмы были доступны развивающимся странам, и организовать соответствующее обучение.

Для того чтобы политика борьбы с киберпреступностью была эффективной и действенной, ее следует строить на доказательственной основе и подвергать строгой оценке. Поэтому на международном уровне следует предпринять целенаправленные и скоординированные усилия для создания механизмов финансирования в целях содействия практическим разработкам и пресечения многих видов вновь появляющихся киберпреступлений. Однако не менее важно, чтобы такие исследования

координировались на международном уровне и чтобы результаты исследований были широкодоступными.

Необходимы оперативные действия на международном уровне, опирающиеся на координацию усилий национальных центров по предупреждению и расследованию транснациональных компьютерных преступлений с аналогичными международными центрами в других странах.

Одним из серьезных шагов направленных на урегулирование этой проблемы явилось принятие Советом Европы 23 ноября 2001 года Конвенции о киберпреступности. Учитывая сложность проблемы, Совет Европы, подготовил и опубликовал проект Конвенции по борьбе с преступлениями в киберпространстве, еще в начале 2000 года. Этот документ стал первым международным соглашением по юридическим и процедурным аспектам расследования и уголовного преследования киберпреступлений. Европейской конвенцией о киберпреступности предусмотрены скоординированные действия на национальном и межгосударственном уровнях, по пресечению несанкционированного вмешательства в работу компьютерных систем, незаконного перехвата данных и вмешательства в компьютерные системы.

Сотрудничество правоохранительных органов различных стран

В процессе проведения расследований правоохранительные органы различных государств должны сотрудничать между собой, причем как официально, используя такие рамки и структуры как, например, Интерпол и др., так и неофициально, предоставляя потенциально полезную информацию непосредственно правоохранительным органам другого государства. В связи с правовой помощью при расследовании киберпреступлений неизбежно будут возникать и другие дополнительные проблемы. Если внутренним правом одной из сторон не предусмотрены конкретные полномочия на поиск доказательств в электронной среде, такая сторона не в состоянии будет адекватно реагировать на просьбу об оказании помощи. По этой причине важным условием международного сотрудничества является согласование полномочий принимать необходимые меры для расследования таких видов преступлений.

Ограниченность национального законодательства и отсутствие единой правовой базы правоохранительных органов в борьбе с этим видом правонарушений – вот одна из главных причин стремительного роста киберпреступности.

Тенденция роста киберпреступности и тенденция "отставания" социально-правового контроля над ней увязываются в некий порочный круг, разорвать который можно только путем органичного сочетания уголовно-правовых и криминалистических стратегий борьбы с этим видом преступлений. Причем важной составляющей такой стратегии должно стать международное сотрудничество в этой сфере, поскольку уже очевидно, что контролировать транснациональную составляющую киберпреступлений на уровне отдельных государств практически невозможно.

Международное сотрудничество в борьбе с преступностью в сфере использования компьютерных технологий нуждается в наличии правового, организационного и научного обеспечения.

Ежегодно происходит усиление угрозы национальной и международной безопасности, которую создает использование науки и техники, особенно компьютерных методов, преступниками и преступными группами. Комплексный характер и широкая распространенность таких методов, используемых при совершении преступлений, диктуют необходимость совместных усилий правительств, гражданского общества и частного сектора. Национальным органам необходимо осознать тот факт, что в случае киберпреступности речь не идет о физическом присутствии на их территории преступников или преступных групп.

Для того чтобы иметь возможность в полной мере сотрудничать друг с другом с учетом транснационального характера преступлений, совершаемых в случае киберпреступности, всем странам необходима надлежащая правовая и оперативная база.

Вот тот комплекс проблем, который вынуждено безотлагательно решать международное сообщество в сфере борьбы с киберпреступностью в XXI веке.

ВЫВОДЫ

Эффективная борьба с киберпреступностью предполагает адекватное выяснение специфики причин ее разрастания. Причем необходимо учитывать и изучать не только данные о преступности, но и данные, характеризующие развитие и изменение других социальных явлений, так или иначе влияющих на преступность: социально-политические явления, организационно-правовые, экономические, демографические и т.д.

Поэтому мы не должны забывать и о том, что в целом преступные проявления имеют единый причинный комплекс, в основе которого находятся наиболее глубокие и острые деформации в обществе во всех его сферах (политической, экономической, социальной и духовной) и на всех его уровнях, начиная с мирового глобального и кончая личностным индивидуальным. Это такие деформации, которые, во-первых, прежде всего выражают несправедливость социального устройства, открывают простор для произвола одних субъектов в ущерб другим; во-вторых, ущемляют права и свободы граждан и, в-третьих, ведут к дегуманизации и ущербности социального статуса и менталитета части населения.

Вот эта ущербность - социальная или нравственно-духовная - и является источником преступного поведения, поскольку она порождает стремление индивида компенсировать свою «неполноценность» за счет других, ценой прав, свобод, здоровья или даже жизни других людей. На мировом уровне новым источником роста социальной напряженности и преступности стала глобализация, поделившая мир на т.н. золотой миллиард, обеспечивающий свое благополучие за счет стран-изгоев с их нищетой, голодом, болезнями и острым стремлением компенсировать свою ущербность или хотя бы отомстить за нее.

Виртуальный мир существенно облегчает это стремление, поскольку позволяет «асимметрично» реагировать на возникающие угрозы. Сегодня любой житель планеты с помощью компьютера, входящего в Сеть, может достаточно легко и пока безнаказанно совершить самое опасное посягательство на всех нас.

Существующее «цифровое неравенство» порождает дефицит и дороговизну компьютерной техники и других средств массовой коммуникации в странах и регионах с неразвитой компьютерной инфраструктурой. Лица, не имеющие возможности платить за доступ в Интернет, иной раз пытаются нелегально подключиться к Сети. В России немало уголовных дел было возбуждено в отношении студентов-математиков, укравших чужие пароли доступа в Интернет.

Широкое распространение пиратской продукции в Китае, Вьетнаме, Индонезии, России и Украине имеет во многом потому, что у пользователей нередко просто нет средств для приобретения этой продукции по более высокой цене.

К сожалению, очевидно, что киберпреступность никуда не исчезнет. В этом нет ничего удивительного. Киберпреступность — не только побочный продукт эпохи интернета, но и часть общего криминального ландшафта. Если что-то можно использовать, то кто-то обязательно найдет возможность использовать это во зло. Компьютерные технологии и интернет — не исключение. Преступность неискоренима, поэтому борьба с киберпреступностью — вопрос не столько «победы в войне», сколько ограничения риска, связанного с работой в интернете.

Для управления этим риском мировому сообществу, несомненно, необходима правовая система вкупе с приспособленными для решения этой задачи и эффективными правоохранительными структурами. Нет сомнения в том, что за последнее десятилетие правоохранительные органы приобрели значительный опыт борьбы с преступлениями в сфере высоких технологий, в том числе и в рамках совместных операций на территории нескольких стран. Для эффективной борьбы с киберпреступностью необходимо дальнейшее сотрудничество, в частности, распространение международного законодательства за пределы развитых стран, а также создание «кибер-Интерпола», который был бы способен преследовать киберпреступников, невзирая на геополитические границы. Это могло бы значительно облегчить борьбу с киберпреступностью.

Отдельные пользователи и компании должны иметь достаточные знания и инструментарий, чтобы свести к минимуму риск стать жертвой киберпреступников. Необходимо выработать разнообразные творческие подходы для повышения уровня понимания обществом проблем, связанных с киберпреступностью и методов, позволяющих уменьшить риск до минимума.

Глава IV

Участники и организация работы Модели Комиссии

А. Подготовка Модели Комиссии

12-19 апреля 2010 года в Сальвадоре (Бразилия) состоится XII Конгресс ООН по предупреждению преступности и уголовному правосудию. В преддверии этого события студенты Международно-правового факультета МГИМО(У) МИД России выступили с инициативой проведения Модели Комиссии по предупреждению преступности и уголовному правосудию в рамках Московской международной модели ООН.

Начинания студентов были поддержаны кафедрой уголовного права, уголовного процесса и криминалистики МГИМО-Университета, Российской ассоциацией содействия ООН, Секретариатом Московской международной модели ООН.

В сентябре 2009 года подготовка к Модели Комиссии начата с выбора повестки дня. Инициативная группа в составе В. Аносовой, Ф. Галеевой, А. Землюковой, Н. Лукоянова, И. Мавлекеева, Е. Путинцевой, Ю. Стахеевой, Б. Штомы и других студентов 3 курса Международно-правового факультета приняла решение о том, что следует обсудить одну из наиболее актуальных тем для современного информационного общества: «Меры по борьбе с преступлениями, связанными с использованием компьютеров».

Организационная работа — поиск аудиторий для заседаний, разработка плаката, печать необходимых для работы Комиссии материалов, а также подготовка доклада, посвященного данному вопросу, включая изучение и анализ существующих нормативно-правовых документов, доктрин, ситуаций с киберпреступностью в мире завершены в ноябре 2009 года.

В. Сроки и место проведения Модели Комиссии

Модель Комиссии по предупреждению преступности и уголовному правосудию, приуроченная к подготовке к двенадцатому Конгрессу Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, проведена в Москве 2-4 декабря 2009 года.

С. Участники Модели Комиссии

В Модели Комиссии приняли участие студенты и магистранты МГИМО(У) МИД России.

<i>Председатель:</i>	Лукоянов Никита Викторович, студент 3 курса Международно-правового факультета (Румыния)
<i>Заместитель Председателя:</i>	Синельник Ксения Александровна, магистрант 1 курса Международного института управления (Аргентина)
<i>Докладчик:</i>	Стахеева Юлия Александровна, студентка 4 курса Международно-правового факультета (Алжир)
<i>Делегаты:</i>	Алферьева Ксения Евгеньевна, студентка 2 курса Международно-правового факультета (Испания)
	Аносова Вероника Хунгяносовна, студентка 3 курса Международно-правового факультета (Буркина-Фасо)
	Астахов Павел Олегович, магистрант 1 курса Международно-правового факультета (Украина)
	Астахова Дарья Олеговна, студентка 2 курса Международно-правового факультета (Литва)
	Галеева Фатима Альбертовна, студентка 3 курса Международно-правового факультета (Коста-Рика)
	Дорохова Екатерина Алексеевна, студентка 3 курса Международно-правового факультета (Германия)
	Землюкова Анастасия Владимировна, студентка 3 курса Международно-правового факультета (Франция)
	Ильчук Александра Владиславовна, студентка 2 курса Международно-правового факультета (Ливан)
	Кержиманкин Вадим Петрович, студент 1 курса Международного института управления (Великобритания)
	Козлова Кристина Валерьевна, студентка 2 курса Международно-правового факультета (Чили)
	Лабуць Дарья Антоновна, студентка 1 курса Международно-правового факультета (ЮАР)
	Мавлекеев Ильсур Шамильевич, студент 3 курса Международно-правового факультета (Бразилия)
	Оленева Оксана Юрьевна, студентка 2 курса Международно-правового факультета (Казахстан)
	Пендечук Галина Васильевна, студентка 4 курса Международно-правового факультета (Катар)
	Прокудина Вероника Павловна, студентка 1 курса Международно-правового факультета (Румыния)
	Супрун Регина Юрьевна, магистрант 1 курса Института европейского права (Канада)
	Тимирясова Ольга Николаевна, студентка 3 курса Международно-правового факультета (Китай)

Черепанов Филипп Олегович, студент 1 курса Международно-правового факультета (Мексика)

Штома Богдана Игоревна, студент 5 курса Международно-правового факультета (США)

D. Открытие Модели Комиссии

Модель Комиссии по предупреждению преступности и уголовному правосудию открыл 2 декабря 2009 года ее Председатель. Он подчеркнул, что впервые проводимая модель Комиссии является эффективным способом стимулирования дискуссии по одной из основных тем двенадцатого Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. Он отметил, что больше внимания необходимо уделять предупреждению преступности как средству устранения ее коренных причин. Выступавший призвал содействовать разработке всеобъемлющих стратегий в целях применения комплексных и многосекторальных подходов к наращиванию потенциала в борьбе с компьютерными преступлениями. При применении таких подходов необходимо уважать права человека, верховенство права и содействовать устойчивому развитию.

Координатор Московской международной модели ООН Ковриженко Г.М. обратился с вступительным словом и отметил роль Председателя модели комиссии и всех заинтересованных проблемой студентов МГИМО(У) МИД России и активное участие в ее подготовке и в предстоящем проведении, отметил значимость участия в модели Комиссии по предупреждению преступности и уголовному правосудию для совершенствования профессиональных навыков будущих юристов-международников.

Профессор кафедры уголовного права, уголовного процесса и криминалистики МГИМО (У) МИД России доктор юридических наук Волеводз А.Г. отметил, что двенадцатый Конгресс знаменует собой пятьдесят пятую годовщину проведения конгрессов Организации Объединенных Наций по предупреждению преступности и уголовному правосудию и может заложить базу для продвижения к цели твердого закрепления центральной роли системы уголовного правосудия в области обеспечения верховенства права и развития. В силу этого проводимой модели следует, как и всему международному сообществу, действовать на основе ранее проделанной работы и идти в ногу со временем.

Генеральный секретарь Московской Международной Модели ООН 2010 года В.Х. Аносова проинформировала участников о целях и задачах Модели, пожелала им успехов в работе.

Заместитель Председателя Модели Комиссии студентка 1 курса магистратуры Международного института управления МГИМО-Университета К.А. Синельник провела тренинг по правилам процедуры Комиссии.

Преподаватель кафедры уголовного права, уголовного процесса и криминалистики МГИМО-Университета В.В. Дубровин проинформировал участников Модели Комиссии о проблеме киберпреступности, основных направлениях в борьбе с ней и ответил на многочисленные вопросы делегатов.

E. Работа Модели Комиссии

В первый день работы Модели Комиссии заслушаны Доклад и выступления делегатов о ситуации, связанной с киберпреступностью, программах и методах борьбы с ней, осуществляемых в рамках отдельных государств. Прошел обмен

мнениями о возможностях и перспективах решения проблемы в общемировом масштабе.

В течение второго дня были продолжены общие прения, по завершению которых Модель Комиссии приступила к разработке и рассмотрению проектов рабочего документа. В Бюро Модели Комиссии поступило два проекта. Оба проекта проверены докладчиком и допущены к обсуждению: разработчики представили их, высказались в пользу принятия или отклонения. По итогам голосования один из проектов стал рабочим, и делегаты приступили к внесению поправок.

Третий день работы Модели Комиссии был посвящен рассмотрению и обсуждению внесенных поправок и голосованию за резолюцию в целом. Именно в последний день работы делегаты смогли испытать на себе всю сложность работы Организации Объединенных Наций. Необходимо было достигнуть общего согласия при обсуждении и координации различных точек зрения, рассмотрении подходов государств всего мира, так как неформальным правилом принятия всех вопросов в Модели Комиссии по предупреждению преступности и уголовному правосудию является достижение консенсуса.

Были обсуждены 22 поправки к рабочему проекту резолюции. Консенсусом приняты 5, остальные 17 поправок отклонены из-за возражений некоторых делегаций.

Е. Принятие Резолюции Модели Комиссии

Однако самым волнующим моментом для всех участников стало принятие резолюции. Председатель внес процедурное предложение принять резолюцию консенсусом. Возражений не поступило.

Резолюция Модели Комиссии одобрена аккламацией, без голосования.

Г. Завершение работы Модели Комиссии

Работа Модели Комиссии завершилась торжественной церемонией закрытия.

Состоялся обмен мнениями о проведенном мероприятии.

Председатель Модели Комиссии Н. В. Лукоянов, выступил с докладом о трехдневной работе Комиссии.

Преподаватель кафедры уголовного права, уголовного процесса и криминалистики МГИМО-Университета В.В. Дубровин поздравил участников Модели Комиссии с успешным завершением ее работы, вручил сертификаты об участии в Модели, а также наградил лучшего делегата по итогам работы Комиссии — Д. О. Астахову, студентку 2 курса Международно-правового факультета.

По итогам работы первой Модели Комиссии среди участников проведено анкетирование, результаты которого показали, что все делегаты оценивают работу в Модели как полезный опыт и имеют намерение продолжать участвовать в Моделях ООН.

Глава V

Резолюция, принятая Моделью Комиссии по предупреждению преступности и уголовному правосудию

Совершенствование мер борьбы с преступлениями, совершаемыми с применением компьютеров

Комиссия по предупреждению преступности и уголовному правосудию,

будучи обеспокоенной тем, что компьютерные сети и электронные ресурсы могут быть использованы для совершения преступлений,

будучи также обеспокоенной серьезной угрозой, которую создают преступления, связанные с использованием компьютерных технологий, для осуществления национальных, региональных и международных проектов в области устойчивого развития и экономического реформирования,

принимая во внимание Европейскую Конвенцию о киберпреступности, которая является в настоящее время единственным международным договором, в котором непосредственно рассматриваются мошенничества и фальсификации, осуществляемые при помощи компьютеров, а также иные виды киберпреступности,

приветствуя все шаги, предпринятые государствами-членами и международными организациями в области борьбы с преступлениями, связанными с использованием компьютерных технологий,

обращая внимание на то, что в настоящее время не выработано единого и универсального определения понятия преступлений, связанных с использованием компьютера,

напоминая, что проблемы киберпреступности приобретают всё большую значимость в связи с развитием компьютерных технологий и ростом числа пользователей сети Интернет,

отмечая несовершенство законодательной базы стран в связи с отсутствием исчерпывающего перечня киберпреступлений и наказаний за данные преступления,

будучи убежденной в необходимости увеличения возможностей для идентификации отдельных лиц в целях предупреждения преступлений, связанных с компьютерными технологиями,

будучи также убежденной в необходимости соблюдения прав человека и неприкосновенности частной жизни от ненадлежащего и противоправного использования,

подчеркивая необходимость создания эффективного международно-правового механизма для борьбы с киберпреступностью,

1. *призывает* государства-члены к сотрудничеству по вопросу разработки более полного и универсального единообразного определения основных понятий, связанных с киберпреступностью;

2. *призывает* все страны, подписавшие Европейскую конвенцию о киберпреступности, ратифицировать её, а также поощряет подписание данного документа странами, не участвовавшими в его подписании, и использование ее опыта в принятии единой международной конвенции о киберпреступности, а также региональных документов;

3. *рекомендует* государствам-членам обеспечить обновление национального законодательства в области уголовного и уголовно-процессуального права, уделив должное внимание вопросам, касающимся определения киберпреступлений, их субъектного состава, следственных полномочий правоохранительных органов, ведущих расследование данных противоправных деяний, и сбора доказательств;

4. *призывает* государства-члены участвовать в разработке единых стандартов в области компьютерной безопасности для правительственных

организаций и частных компаний, работа которых связана с информационной и национальной безопасностью;

5. *призывает* правоохранительные органы государств-членов сотрудничать по вопросам выявления, предупреждения, пресечения, расследования киберпреступлений, по вопросам выдачи и наказания лиц, виновных в совершении таких преступлений, а также по вопросам повышения качества потенциала и квалификации специалистов;

6. *рекомендует* государствам-членам оптимизировать функционирование научно-исследовательских центров по вопросам киберпреступности, в частности посредством обеспечения их надлежащего финансирования, и усилить сотрудничество между данными центрами как на национальном, так и на международном уровнях;

7. *поощряет* сотрудничество между научно-исследовательскими центрами, экспертными учреждениями, а также специалистами по уголовному праву, процессу и криминалистике по вопросам квалификации компьютерных преступлений, разработке методики, техники и тактике их предупреждения, пресечения и расследования;

8. *поощряет* сотрудничество стран в области разработки и производства специального компьютерного оборудования в целях борьбы с киберпреступностью;

9. *поощряет* сотрудничество стран на различных уровнях с целью обмена опытом в области борьбы с киберпреступлениями;

10. *призывает* государства-члены опубликовывать ежегодные статистические отчеты о количестве зарегистрированных и раскрытых киберпреступлений;

11. *поощряет* разработку общеобразовательных и специальных программ подготовки специалистов по компьютерным технологиям, информационному праву и борьбе с киберпреступлениями для средних и высших учебных заведений;

12. *призывает* государства-члены проводить мероприятия по разработке эффективного механизма помощи государствам, пострадавшим от атак в сети Интернет, с целью их применения в случае, если пострадавшее государство запросит помощи;

13. *призывает* страны принять меры, направленные на повышение уровня осведомленности населения, в частности, посредством проведения профилактических мероприятий, повышения квалификации специалистов системы органов уголовного правосудия и лиц, ответственных за разработку политики в этой области;

14. *постановляет* продолжать активно заниматься этим вопросом.