



Отдел проблем экономической преступности
Генеральный директорат по
правам человека и правовым вопросам
Страсбург, Франция
2 апреля 2008 года

**Руководящие принципы
сотрудничества
правоохранительных органов и
провайдеров услуг сети Интернет
против компьютерных преступлений**

приняты глобальной Конференцией
"Сотрудничество против компьютерной преступности"
Совет Европы, Страсбург, 1-2 апреля 2008 года

Эти руководящие принципы – результат нескольких раундов дискуссий, состоявшихся в период с октября 2007 года по февраль 2008 года между представителями отрасли и правоохранительными органами при содействии "Проекта против компьютерных преступлений" Совета Европы. Их дополнением служит подробная историческая справка.

Настоящие руководящие принципы впоследствии явились предметом обсуждения и были утверждены участниками глобальной Конференции "Сотрудничество против компьютерных преступлений" (Совет Европы, Страсбург, Франция), состоявшейся 1-2 апреля 2008 года.

Настоящие руководящие принципы не имеют обязательной силы и являются средством, которое может распространяться и использоваться с целью содействия правоохранительным органам и поставщикам услуг в любой стране мира в организации их сотрудничества в сфере противодействия компьютерным преступлениям, обеспечивая уважение к их функциям и обязанностям, а также прав пользователей сети Интернет.

Руководящие принципы сотрудничества правоохранительных органов и поставщиков услуг сети Интернет против компьютерных преступлений¹

Вступление

1. Построение информационного общества требует укреплять доверие в сфере информационно-коммуникационных технологий (ИКТ), защищать личные данные и тайну частной жизни и формировать всеохватывающую культуру компьютерной безопасности в обстоятельствах все большей зависимости общества от ИКТ и, таким образом, его уязвимости для компьютерной преступности.

2. Участники Первой и Второй всемирных встреч на высшем уровне, посвященных информационному обществу (Женева 2003 г., Тунис 2005 г.), кроме прочего, взяли на себя обязательство строить информационное общество для всех, в котором каждый сможет создавать, получать доступ, использовать и обмениваться информацией и знаниями, реализовать свой потенциал и повышать качество своей жизни, основываясь на целях и принципах Устава Организации Объединенных Наций, полностью соблюдая и подтверждая положения Всеобщей декларации прав человека, что требует новых форм сотрудничества и взаимодействия между правительствами, частным сектором, гражданским обществом и международными организациями.

3. Важную роль в реализации этой перспективы играют поставщики услуг сети Интернет (ПУИ) и правоохранительные органы (ПОО).

4. Национальное законодательство, соответствующее Конвенции о компьютерных преступлениях Совета Европы ("Будапештская конвенция"), способствует странам в создании прочной правовой базы для сотрудничества между государственным и частным секторами, следственных полномочий, а также международного сотрудничества.

5. Руководящие принципы, не ставя цели подменить собой существующий правовой инструментарий, предполагают существование соответствующих юридических документов, предусматривающих сбалансированную систему средств для проведения расследования с соблюдением соответствующих гарантий и механизмов защиты таких основных прав человека, как свобода выражение взглядов, тайна личной жизни, жилища и корреспонденции и право на защиту данных. Таким образом, с целью всесторонней имплементации процессуальных норм Конвенции о компьютерных преступлениях государствам рекомендуется закрепить соответствующие положения в системе внутригосударственного права, определить следственные органы и обязательства правоохранительных органов, установив условия и гарантии, предусмотренные в Статье 15 Конвенции. Это

- обеспечит гарантии эффективной работы правоохранительных органов
- защитит возможность поставщиков услуг сети Интернет оказывать услуги
- обеспечит соответствие национальных норм глобальным стандартам
- будет способствовать утверждению глобальных стандартов, а не изолированных национальных решений
- будет содействовать обеспечению надлежащей правовой процедуры и верховенства права, включая принципы законности, пропорциональности и необходимости.

6. Для целей этих руководящих принципов используется включенное в Статью 1 Конвенции о компьютерной преступности широкое определение поставщика услуг, согласно которому таковым является:

- i. любая государственная или частная структура, которая обеспечивает пользователям ее услуг возможность обмена информацией посредством компьютерной системы, и
- ii. любая другая структура, которая осуществляет обработку или хранение компьютерных данных от имени такой службы связи или пользователей такой службы.

7. С целью усиления безопасности в киберпространстве, сведения до минимума использования услуг в незаконных целях и укрепления доверия в сфере ИКТ, существенно, чтобы поставщики услуг сети Интернет и правоохранительные органы эффективно взаимодействовали друг с другом, надлежащим образом, учитывая их соответствующие функции, издержки, связанные с таким взаимодействием, и права граждан.

¹ Данный документ необязательно отображает официальную позицию Совета Европы. Для получения дополнительной информации следует обращаться к: Alexander.seger@coe.int

8. Данные принципы нацелены на оказание помощи правоохранительным органам и поставщикам услуг сети Интернет в систематизации их взаимодействия в вопросах компьютерной преступности. В основу их легли примеры надлежащей практики, с тем, чтобы быть применимыми в любой стране мира с учетом ее национального законодательства и с соблюдением гарантий свободы выражения взглядов, частной жизни, защиты персональных данных и других основных прав граждан.

9. Таким образом, государствам, правоохранительным органам и поставщикам услуг сети Интернет рекомендуется принять следующие меры на общегосударственном уровне:

Общие руководящие принципы

10. Правоохранительные органы и поставщиков услуг сети Интернет следует поощрять в обмене информацией с целью усиления их способности выявлять и противодействовать тем видам компьютерной преступности, которые находятся на стадии становления. Правоохранительные органы следует поощрять в информировании поставщиков услуг о тенденциях в сфере компьютерной преступности.

11. Правоохранительным органам и поставщикам услуг сети Интернет следует способствовать развитию культуры сотрудничества, а не конфронтации, включая обмен надлежащей практикой. Поощряется проведение регулярных встреч для обмена опытом и поиска решений существующих проблем.

12. Правоохранительные органы и поставщиков услуг следует поощрять в разработке письменных процедур взаимодействия. По возможности, обе стороны следует поощрять в предоставлении друг другу структурированной информации об эффективности таких процедур.

13. Следует изучить возможность создания официальных форм сотрудничества между правоохранительными органами и поставщиками услуг с целью установления долгосрочных отношений с обеспечением обеих сторон надлежащими гарантиями относительно того, что такое сотрудничество не будет ущемлять законных прав представителей отрасли и нарушать каких-либо законных полномочий правоохранительных органов.

14. Как правоохранительным органам, так и поставщикам услуг сети Интернет надлежит защищать основные права граждан в соответствии со стандартами Объединенных Наций и другими соответствующими европейскими и международными стандартами. К этим стандартам относятся Конвенция Совета Европы 1950 года о защите прав человека и основных свобод, Международный пакт о гражданских и политических правах Организации Объединенных Наций 1966 года, Конвенция Совета Европы 1981 о защите лиц в связи с автоматизированной обработкой персональных данных. А также - нормам внутригосударственного права. Эти требования накладывают разумные ограничения на возможный объем сотрудничества.

15. Поощряется взаимное сотрудничество правоохранительных органов и поставщиков услуг сети Интернет с целью осуществления контроля по соблюдению стандартов защиты частной жизни и защиты данных на национальном уровне, а также в связи с трансграничными потоками данных. Руководством в этом отношении является деятельность Совета Европы и ОЕСР.

16. Обе стороны должны принимать во внимание затраты, связанные с формированием запросов и предоставлением ответов на них. Финансовые последствия соответствующих мероприятий следует учитывать при разработке процедур. Также необходимо рассмотреть вопрос возмещения затрат или справедливой компенсации соответствующим сторонам.

Меры, которые следует принять правоохранительным органам

17. Широкое, стратегическое сотрудничество – Следует поощрять правоохранительные органы в оказании содействия поставщикам услуг путем осуществления стратегического взаимодействия с предприятиями соответствующей отрасли. Сюда входит проведение регулярных учебных семинаров по технической и правовой тематике, а также предоставление информации о расследованиях, проводимых на основании жалоб от поставщиков услуг, или оперативных данных об известной преступной деятельности, предоставленными поставщиками услуг.

18. Процедуры, связанные с юридически обязательными запросами – Следует рекомендовать правоохранительным органам разработать письменные процедуры, включая соответствующие меры должной осмотрительности, для направления и обработки юридически обязательных запросов, и обеспечить выполнение запросов в соответствии с установленным порядком.

19. Профессиональная подготовка – Правоохранительным органам следует рекомендовать обеспечить профессиональную подготовку определенного круга сотрудников по вопросам осуществления этих процедур, включая способ получения учетно-отчетных материалов от

поставщиков услуг, обработки полученной информации, а также по вопросам интернет-технологий и влияния, которые они оказывают в целом, соблюдения надлежащей правовой процедуры и основных прав человека.

20. Технические ресурсы – Сотрудники правоохранительных органов, отвечающие за взаимодействие с поставщиками услуг, должны обеспечить себя необходимыми техническими ресурсами, включая доступ к Интернету, ведомственный адрес электронной почты, обнаруживающий связь с ведомством, и другие технические средства, которые позволят им в безопасном режиме получать информацию от поставщика услуг в электронном виде.

21. Назначенный персонал и контактные центры – Сотрудничество между правоохранительными органами и поставщиками услуг следует ограничить квалифицированным персоналом. Необходимо поддержать правоохранительные органы в определении контактных центров для осуществления сотрудничества с поставщиками услуг.

22. Орган для направления запросов – Правоохранительным органам следует рекомендовать четко определить в своих письменных процедурах сотрудников, уполномоченных давать разрешение на применение соответствующих – и каких именно – мер в отношении поставщиков услуг сети Интернет, направлять им запросы. Также им необходимо определить, каким образом поставщики услуг сети Интернет смогут проверять /подтверждать подлинность этих запросов.

23. Правоохранительным органам следует рекомендовать информировать поставщиков услуг сети Интернет о своих процедурах и, по возможности, о том, кто из сотрудников конкретно или какие конкретно должности назначены ответственным за сотрудничество с поставщиками услуг сети Интернет.

24. Проверка источника запроса – Источник запроса, направляемого из правоохранительных органов, должен поддаваться проверке со стороны поставщиков услуг:

- вся корреспонденция должна включать имя контактного лица, номер телефона и адрес электронной почты сотрудника (-ов) правоохранительного органа, ведущего поиск учетно-отчетных материалов, с тем, чтобы поставщик услуг в случае возникновения вопросов мог связаться с запрашивающим лицом
- поставщиков услуг следует просить вести переписку с сотрудником не по личному адресу электронной почты сотрудника, а пользоваться соответствующей учетной записью ведомственной электронной почты
- все письма следует направлять на официальном бланке ведомства, причем любая корреспонденция должна включать номер главного коммутатора ведомства и адрес его веб-сайта с тем, чтобы поставщики услуг могли предпринять шаги для проверки подлинности запросов, если сочтут необходимым.

25. Запросы – Запросы правоохранительных органов поставщикам услуг следует оформлять в письменном виде (или в юридически приемлемом электронном виде) с документальным подтверждением. В особо срочных случаях, допускающих устный запрос, следует после немедленно оформить их в письменной (или иной юридически приемлемой электронной) форме.

26. Стандартная форма запроса – Правоохранительным органам на национальном и, если возможно, на международном уровне следует рекомендовать стандартизировать и систематизировать форму, используемую для направления запросов и реагирования на них. Запрос должен содержать, как минимум, следующую информацию:

- Регистрационный номер
- Ссылка на правовое основание
- Конкретные запрашиваемые данные
- Сведения для проверки источника запроса

27. Конкретность и точность запросов – Правоохранительным органам следует рекомендовать обеспечить конкретность, полноту и четкость направляемых запросов и с достаточной их детализацией, чтобы поставщики услуг могли определять данные, имеющие отношение к делу. Им следует рекомендовать направлять запросы тому поставщику услуг, в распоряжении которого находятся учетно-отчетные материалы. Следует избегать запросов о предоставлении многокомпонентных и неконкретных данных.

28. Правоохранительные органы следует поощрять в предоставлении как можно большего количества фактов расследования, без ущерба для самого расследования или каких-либо основных прав, чтобы содействовать поставщикам услуг в идентификации соответствующих данных.

29. Правоохранительным органам следует рекомендовать предоставлять поставщикам услуг пояснения о несвязанных с конкретным делом методах расследования, чтобы последние понимали,

как сотрудничество с их стороны способствует более эффективному расследованию преступлений и лучшей защите граждан.

30. Определение приоритетности – Правоохранительным органам следует рекомендовать установить приоритетность запросов, особенно связанных с большими объемами данных, чтобы поставщики услуг могли обрабатывать в первую очередь наиболее важные. Определять приоритетность лучше всего согласованно во всех правоохранительных органах на общегосударственном и, если возможно, международном уровне.

31. Целесообразность запросов – Правоохранительным органам следует рекомендовать принимать во внимание издержки, несущие поставщиками услуг в связи с запросами, и предоставлять поставщикам услуг достаточно времени для реагирования на них. Они должны помнить о том, что поставщики услуг, возможно, должны реагировать на запросы, поступающие из других правоохранительных органов, и стремиться к тщательному отслеживанию представляемых объемов.

32. Конфиденциальность данных – Правоохранительным органам следует гарантировать конфиденциальность получаемых данных.

33. Избегать ненужных затрат и нарушения деловых операций – Правоохранительным органам следует рекомендовать избегать ненужных затрат и нарушения деловых операций поставщиков услуг и других субъектов хозяйственной деятельности.

34. Правоохранительным органам следует рекомендовать ограничить использование службы чрезвычайных контактных центров наиболее срочными случаями во избежание злоупотребления.

35. Правоохранительные органы следует поощрять к обеспечению своевременного издания постановлений о предъявлении информации после постановлений о сохранности или своевременному уведомлению поставщика услуг сети Интернет об отсутствии необходимости в дальнейшем сохранении данных.

36. Международные запросы – В случае направления запросов поставщикам услуг сети Интернет, находящимся за пределами государства, национальным правоохранительным органам следует рекомендовать не направлять запросы таким поставщикам услуг сети Интернет непосредственно, а пользоваться процедурами, описанными в международных соглашениях, таких как Конвенция о компьютерных преступлениях, а также в случае срочных мер, включая постановления о сохранности/запросы, также сетью круглосуточно работающих контактных центров правоохранительных органов.

37. Запросы о международной взаимной помощи – Правоохранительным органам и органам уголовного судопроизводства следует рекомендовать принятие необходимых мер с целью обеспечения того, что за запросами о временных мерах следуют международные процедуры в сфере взаимной юридической помощи, или что поставщики услуг сети Интернет своевременно уведомляются об отсутствии необходимости в дальнейшем сохранении данных.

38. Координация между правоохранительными органами – правоохранительным органам следует рекомендовать координировать их взаимодействие с поставщиками услуг сети Интернет и осуществлять взаимный обмен передовой практикой как на национальном, так и на международном уровне. На международном уровне им с этой целью следует использовать соответствующие международные представительства.

39. Программы контроля соблюдения уголовно-правовых норм – Правоохранительные органы следует поощрять в организации изложенных выше видов взаимодействия с поставщиками услуг в форме комплексной программы контроля соблюдения уголовно-правовых норм с предоставлением поставщикам услуг описания такой программы, включая:

- информацию, необходимую для установления связи с назначенным персоналом правоохранительных органов, отвечающим за программу контроля соблюдения уголовно-правовых норм, а также сведения о режиме работы такого персонала
- информацию, необходимую для предоставления поставщиком услуг документов персоналу, отвечающему за соблюдение уголовно-правовых норм
- другие подробности, имеющие отношение к правоохранителям, отвечающих за соблюдения уголовно-правовых норм (например, объем сотрудничества правоохранительных органов с другими странами, документы, подлежащие переводу на какой-либо язык и т.д.).

40. Аудит системы контроля соблюдения – Правоохранительным органам следует рекомендовать осуществлять контроль и проверку системы обработки запросов в статистических целях, в том

числе с целью определения ее сильных и слабых сторон и, если необходимо, публиковать ее результаты.

Меры, которые следует принять поставщикам услуг

41. Сотрудничество с целью минимизации использования услуг с неправомерной целью – При условии соблюдения применимых прав и свобод, таких как свобода слова, неприкосновенность частной жизни и других норм государственного или международного права, а также условий соглашений с пользователями, поставщикам услуг следует рекомендовать сотрудничать с правоохранительными органами с целью сведения к минимуму возможности использования услуг в преступной деятельности, как это определено законом.

42. Поставщикам услуг следует рекомендовать уведомлять правоохранительные органы о становящихся им известными случаях с уголовно-правовыми последствиями, затрагивающих поставщика услуг сети Интернет, однако это не обязывает поставщиков услуг предпринимать активные меры для выявления фактов или обстоятельств, указывающие на такие противозаконные действия.

43. Поставщикам услуг следует рекомендовать содействовать правоохранительным органам в осуществлении образовательных, обучающих мероприятий и других формах поддержки их услуг и деятельности.

44. Реагирование на запросы из правоохранительных органов – Поставщикам услуг следует рекомендовать прилагать все обоснованные усилия для оказания содействия правоохранительным органам в исполнении запроса.

45. Порядок реагирования на запросы – Поставщиков услуг следует поощрять в разработке письменных процедур, включая соответствующие меры по должному усердию, для обработки запросов, а также в обеспечении соответствия согласованным процедурам их ответов на запросы.

46. Обучение – Поставщикам услуг следует рекомендовать обеспечить обучение в достаточном объеме персонала, ответственного за осуществление этих процедур.

47. Назначенный персонал и контактные центры – Поставщикам услуг следует рекомендовать назначить в качестве контактных центров (лиц) для сотрудничества с правоохранительными органами квалифицированный персонал

48. Помощь в чрезвычайных ситуациях – Поставщикам услуг следует рекомендовать предусмотреть средство, дающее правоохранительным органам возможность связываться с их сотрудниками, отвечающими за контроль соблюдения уголовно-правовых норм, вне обычного рабочего времени с целью реагирования на чрезвычайные ситуации. Поставщикам услуг следует рекомендовать предоставить правоохранительным органам соответствующую информацию для оказания помощи в чрезвычайных ситуациях.

49. Ресурсы – Поставщикам услуг следует рекомендовать предоставить в распоряжение своих контактных центров или персонала, ответственного за сотрудничество с правоохранительными органами, те ресурсы, которые им необходимы для выполнения запросов правоохранительных органов.

50. Программы контроля соблюдения уголовно-правовых норм – Поставщикам услуг следует рекомендовать организовать их сотрудничество с правоохранительными органами в форме комплексных программ контроля соблюдения уголовно-правовых норм, предоставив правоохранительным органам описание таких программ, включая:

- информацию, необходимую для осуществления связи с назначенным персоналом поставщиков, ответственным за контроль соблюдения уголовно-правовых норм, а также режим работы такого персонала;
- информацию, необходимую для того, чтобы правоохранительные органы могли предоставлять документы персоналу, отвечающему за контроль соблюдения уголовно-правовых норм;
- прочие подробные сведения, имеющие отношение к персоналу поставщиков, отвечающему за контроль соблюдения уголовно-правовых норм (такие как объем деятельности поставщика услуг в других странах, документы, подлежащие переводу на какой-либо язык и т.д.);
- с целью обеспечения возможности правоохранительных органов направлять конкретные и уместные запросы поставщикам услуг следует рекомендовать предоставить информацию о типе услуг, предлагаемых ими пользователям, включая гиперссылки на услуги во всемирной

сети Интернет и дополнительные сведения, а также ссылку на контактное лицо для получения дополнительной информации;

- поставщику услуг сети Интернет следует, по возможности, рекомендовать предоставлять в ответ на запрос перечень категорий данных, которые могли бы предоставляться правоохранительным органам по каждой услуге в случае получения имеющего силу запроса правоохранительных органов о раскрытии информации, имея в виду то, что не всегда при проведении конкретного уголовного расследования такие данные будут иметься в распоряжении.

51. Проверка источника запросов – Поставщикам услуг следует рекомендовать предпринять шаги для осуществления, в пределах их возможностей и по мере необходимости, проверки подлинности запросов, поступающих из правоохранительных органов, с целью предотвратить разглашение содержания учетно-отчетных материалов об их клиентах неуполномоченным лицам.

52. Ответы – Поставщикам услуг следует рекомендовать отвечать на запросы правоохранительных органов в письменном (или другом юридически приемлемом электронном) виде, обеспечивая наличие документального подтверждения относительно таких запросов и ответов, имея в виду то, что данный след может и не содержать персональные данные.

53. Стандартная форма ответа – Принимая во внимание форму запроса, используемую правоохранительными органами, поставщикам услуг следует рекомендовать стандартизировать форму направления информации правоохранительным органам.

54. Поставщикам услуг следует рекомендовать обрабатывать запросы своевременно, в соответствии с определенными ими письменными процедурами, проинформировав правоохранительные органы о среднем времени задержки, связанной с направлением ответа на запросы.

55. Подтверждение направленной информации – Поставщикам услуг следует рекомендовать обеспечить полноту, точность и защищенность информации, направляемой правоохранительным органам.

56. Конфиденциальность запросов – Поставщикам услуг следует гарантировать конфиденциальность получаемых запросов.

57. Разъяснения относительно непредоставленной информации – Поставщикам услуг следует рекомендовать в случае отклонения запросов или невозможности предоставления информации представлять запрашивающему правоохранительному органу соответствующие разъяснения.

58. Аудит системы контроля соблюдения – Поставщикам услуг следует рекомендовать осуществлять контроль и проверку системы обработки запросов в статистических целях с тем, чтобы определять ее сильные и слабые стороны, и в соответствующих случаях публиковать полученные результаты.

59. Координация между поставщиками услуг – поставщикам услуг с соблюдением антимонопольных норм/правил конкуренции следует рекомендовать координировать свое взаимодействие с правоохранительными органами обмениваться друг с другом позитивной практикой, используя с этой целью профессиональные объединения поставщиков услуг.