Проект проти кіберзлочинності
www.coe.int/cybercrime

Відділ проблем економічної злочинності
Генеральний директорат з
прав людини та правових питань
Страсбург, Франція
2 квітня 2008 року

Керівні принципи співробітництва між правоохоронними органами та постачальниками послуг мережі Інтернет проти кіберзлочинності

Ухвалені глобальною Конференцією
"Співробітництво проти кіберзлочинності"
Рада Європи, Страсбург, 1-2 квітня 2008 року

Ці керівні принципи – результат декількох раундів дискусій між представниками підприємств і правоохоронних органів, що відбулися в період з жовтня 2007 року по лютий 2008 року під патронатом "Проекту проти кіберзлочинності" Ради Європи. Їх доповнює детальна історична довідка.

До того ж ці керівні принципи були обговорені й ухвалені на глобальній Конференції "Співробітництво проти кіберзлочинності" (Рада Європи, Страсбург, Франція) 1-2 квітня 2008 року.

Керівні принципи є необов'язковими за своїм характером, і можуть поширюватися та використовуватися як засіб, що допомагає правоохоронним органам і постачальникам послуг у будь-якій країні світу в організації співпраці, спрямованої на протидію кіберзлочинності, поважаючи їхні відповідні ролі та обов'язки, а також прав користувачів мережі Інтернет.

Керівні принципи співробітництва між правоохоронними органами й постачальниками послуг мережі Інтернет проти кіберзлочинності[1]

Вступ

1. Побудова інформаційного суспільства потребує зміцнення довіри в сфері інформаційно-комунікаційних технологій (ІКТ), захисту персональних даних і таємниці приватного життя та формування глобальної культури комп'ютерної безпеки в зв'язку з тим, що суспільство в усьому світі виявляє дедалі більшу залежність від ІКТ і, таким чином, уразливість для кіберзлочинності.

2. Учасники Першого та Другого всесвітніх саммітів, присвячених інформаційному суспільству (Женева 2003 р., Туніс 2005 р.), крім іншого, зобов'язалися будувати інформаційне суспільство для всіх, у якому кожен могтиме створювати інформацію та знання, мати до них доступ, використовувати їх і обмінюватися ними, реалізувати свій потенціал і підвищувати якість свого життя, виходячи з цілей і принципів Статуту Організації Об'єднаних Націй, у повній мірі дотримуючись і підтверджуючи положення Загальної декларації прав людини, що вимагає нових форм взаємодії й співробітництва між урядами, приватним сектором, громадянським суспільством і міжнародними організаціями.

3. Визначну роль у реалізації цієї перспективи відіграють постачальники послуг мережі Інтернет (ППІ) і правоохоронні органи (ПОО).

4. Національне законодавство, що відповідає Конвенції про кіберзлочинність Ради Європи ("Будапештська конвенція"), сприяє країнам у створенні міцної правової бази для співробітництва між публічним і приватним секторами, слідчих повноважень, а також міжнародної співпраці.

5. Керівні принципи не мають на меті замінити існуючу правову базу, але припускають існування відповідних правових документів, які передбачають збалансовану систему засобів розслідування з відповідними гарантіями й механізмом захисту таких основних прав людини, таких як свобода вираження поглядів, таємниця особистого життя, житла й кореспонденції й право на захист даних. Тому для повної імплементації процесуальних норм Конвенції про кіберзлочинність державам рекомендується затвердити положення в системі національного права, щоб визначити слідчі органи й зобов'язання правоохоронних органів, установивши умови й гарантії, передбачені в Статті 15 Конвенції. Це

- гарантуватиме ефективну роботу правоохоронних органів
- захищатиме можливість постачальників послуг мережі Інтернет надавати послуги
- гарантуватиме відповідність національних норм світовим стандартам
- сприятиме утвердженню світових стандартів замість ізольованих національних рішень
- сприятиме забезпеченню належної правової процедури й утвердженню верховенства права, включаючи принципи законності, пропорційності й необхідності.

6. Для цілей цих керівних принципів застосовується подане в статті 1 Конвенції про кіберзлочинність широке визначення "постачальника послуг", згідно з яким такий означає:

i будь-яку публічну або приватну установу, яка надає користувачам своїх послуг можливість комунікацій за допомогою комп'ютерної системи, та

ii будь-яку іншу установу, яка обробляє або зберігає комп'ютерні дані від імені такої комунікаційної послуги або користувачів такої послуги.

[1] Цей документ необов'язково відображає офіційну позицію Ради Європи. Для отримання додаткової інформації звертайтеся до: Alexander.seger@coe.int

7. З метою підсилення кібербезпеки, зведення до мінімуму можливості використання послуг у протиправних цілях і зміцнення довіри в сфері ІКТ, вкрай важливо, щоб постачальники послуг мережі Інтернет і правоохоронні органи ефективно співпрацювали, належним чином враховуючи їхні відповідні функції, витрати, пов'язані з такою співпрацею, а також права громадян.

8. Мета цих керівних принципів полягає в тому, щоб надати допомогу правоохоронним органам і постачальникам послуг мережі Інтернет у систематизації форм їхньої взаємодії, пов’язаних із проблематикою кіберзлочинності. Вони спираються на існуючі приклади передової практики і мають застосовуватися в будь-якій країні світу з урахуванням національного законодавства та з дотриманням гарантій свободи вираження поглядів, приватного життя, захисту даних особистого характеру і інших основних прав громадян.

9. З огляду на це державам, правоохоронним органам і постачальникам послуг мережі Інтернет рекомендовано вжити на загальнодержавному рівні таких заходів:

Загальні керівні принципи

10. Правоохоронні органи й постачальників послуг мережі Інтернет слід заохочувати до участі в обміні інформацією з метою зміцнення їхньої здатності виявляти види комп'ютерної злочинності, які перебувають ще на стадії становлення, і протидіяти їм. Правоохоронні органи слід заохочувати інформувати постачальників послуг про різні тенденції в сфері комп'ютерної злочинності.

11. Правоохоронним органам і постачальникам послуг мережі Інтернет слід прагнути до співробітництва, радше ніж до протистояння, включаючи обмін передовою практикою. Необхідно заохочувати проведення регулярних зустрічей для обміну досвідом і розв’язання проблем.

12. Правоохоронні органи й постачальників послуг слід заохочувати до розробки письмових процедур взаємодії. В випадках, коли це можливо, слід заохочувати обидві сторони до обміну інформацією щодо застосування цих процедур.

13. Слід вивчити можливість встановлення офіційних форм взаємодії між правоохоронними органами й постачальниками послуг з метою побудови довгострокових відносин з належними гарантіями того, що така співпраця не порушить законних прав інтернет-індустрії та будь-яких закріплених у законі повноважень правоохоронних органів.

14. Як правоохоронним органам, так і постачальникам послуг мережі Інтернет слід захищати основні права громадян згідно зі стандартами Об'єднаних Націй і іншими застосовними європейськими й міжнародними стандартами, такими як Конвенція Ради Європи 1950 року "Про захист прав людини й основоположних свобод", Міжнародний пакт Організації Об'єднаних Націй про цивільні й політичні права 1966 року, Конвенція Ради Європи 1981 року "Про захист осіб у зв’язку з автоматизованою обробкою даних особистого характеру", а також згідно із внутрішньодержавним правом. Це накладає обґрунтовані обмеження на можливе співробітництво.

15. Заохочується співпраця правоохоронних органів і постачальників послуг мережі Інтернет з метою контролю за дотриманням стандартів захисту приватного життя й захисту даних на національному рівні, а також щодо транскордонних потоків даних. Загальне спрямування цій співпраці надає діяльність Ради Європи й ОЕСР.

16. Обидві сторони мають усвідомлювати, що формування запитів і надання відповідей на них пов’язане з витратами. Слід ураховувати фінансові наслідки цих заходів при розробці процедур та розглянути питання відшкодування витрат або справедливої компенсації відповідним сторонам.

Заходи, яких слід ужити правоохоронним органам

17. Широке, стратегічне співробітництво – Правоохоронним органам слід порекомендувати допомагати постачальникам послуг, беручи участь у широкому, стратегічному співробітництві з інтернет-індустрією, включно з проведенням регулярних навчальних семінарів з технічних і правових питань, а також інформуючи про розслідування, здійснені на підставі скарг, надісланих постачальниками послуг, або оперативних даних, зібраних щодо явно злочинної діяльності, про яку повідомили постачальники послуг.

18. Процедури, пов'язані з юридично обов'язковими запитами – Правоохоронним органам слід рекомендувати розробити письмові процедури, включно з відповідними заходами належної обачності, для спрямування й обробки юридично обов'язкових запитів та забезпечення виконання запитів відповідно до погодженого порядку.

19. Професійна підготовка – Правоохоронним органам слід рекомендувати забезпечити професійну підготовку визначеного кола своїх працівників з питань здійснення цих процедур, включаючи спосіб отримання облікових матеріалів (records) від постачальників послуг, обробки отриманої інформації, а також інтернет-технологій і їхнього впливу в цілому, а також дотримання належної правової процедури й основоположних прав людей.

20. Технічні ресурси – Працівникам правоохоронних органів, відповідальним за співпрацю з постачальниками послуг, слід надати в розпорядження необхідні технічні ресурси, включаючи доступ до мережі Інтернет, відомчу адресу електронної пошти, що наочно виявляє зв'язок із відомством, та інші технічні засоби, які їм дозволять безпечно одержувати інформацію від постачальника послуг в електронній формі.

21. Визначений персонал і органи для здійснення контактів – Взаємодія між правоохоронними органами і постачальниками послуг має бути обмежена кваліфікованим персоналом. Для співробітництва з постачальниками послуг правоохоронним органам слід рекомендувати визначити органи для здійснення контактів.

22. Орган для спрямування запитів – Правоохоронні органи слід заохочувати до того, щоб у своїх письмових процедурах вони чітко визначили, хто з працівників правоохоронних органів уповноважений давати санкцію на застосування заходів – і яких саме заходів – щодо постачальників послуг мережі Інтернет, надсилати їм запити, і яким чином постачальники послуг мережі Інтернет можуть перевіряти /підтверджувати справжність цих запитів.

23. Правоохоронні органи слід заохочувати до інформування постачальників послуг мережі Інтернет про свої процедури й, по змозі, про те, хто з працівників або кого за посадою призначено відповідати за співробітництво з постачальниками послуг мережі Інтернет.

24. Перевірка джерела запиту – Джерело запиту, що направляється з правоохоронних органів, має вможливлювати перевірку з боку постачальників послуг:

- Уся кореспонденція має включати найменування контактної особи, номер телефону й адресу електронної пошти працівника (-ів) правоохоронного органа, що розшукує облікові матеріали, аби постачальник послуг міг зв'язатися із запитуючою особою у разі виникнення питань
- Постачальників послуг слід просити надсилати кореспонденцію працівникові не на особисту адресу електронної пошти працівника, а на відповідний обліковий запис відомчої електронної пошти
- Усі листи слід направляти на офіційному бланку відомства, і в усій кореспонденції належить зазначати номер головного комутатора відомства й адресу його веб-сайту, аби постачальники послуг могли вжити заходів для перевірки справжності запитів, якщо вважатимуть це за потрібне.

25. Запити – Запити правоохоронних органів постачальникам послуг слід оформляти в письмовій формі (або в іншій юридично прийнятній електронній формі) із забезпеченням документального сліду. У вкрай термінових випадках, коли прийнятними є усні запити, у їхній розвиток належить негайно направляти документи в письмовій (або іншій юридично прийнятній електронній) формі.

26. Стандартна форма запиту – Правоохоронні органи на національному та, по змозі, на міжнародному рівні слід заохочувати до стандартизації й систематизації форми, використовуваної для спрямування запитів і реагування на них. Запити мають містити принаймні наступну інформацію:

- Реєстраційний номер
- Посилання на правову підставу
- Конкретні запитувані дані
- Відомості для перевірки джерела запиту

27. Конкретність і точність запитів – Правоохоронні органи слід заохочувати до забезпечення конкретності, повноти й чіткості спрямованих запитів і достатнього ступеня їх деталізації для того, щоб постачальники послуг могли визначити дані, стосовні до справи. Їм слід рекомендувати забезпечити спрямування запитів тому постачальникові послуг, який має в своєму розпорядженні облікові матеріали. Слід уникати запитів про надання багатокомпонентних і неконкретних даних.

28. Правоохоронні органи слід заохочувати до надання якомога більшої кількості фактів про розслідування, проте без шкоди для самого розслідування або будь-яких основоположних прав, аби дозволити постачальникам послуг визначити дані, стосовні до справи.

29. Правоохоронні органі слід заохочувати до надання постачальникам послуг пояснень і допомоги щодо методів розслідування, не пов'язаних зі справою, аби останні розуміли, як співробітництво з їхнього боку сприяє ефективнішому розслідуванню злочинів і кращому захистові громадян.

30. Визначення пріоритетності – Правоохоронним органам слід рекомендувати встановлювати пріоритетність запитів, а надто пов'язаних з більшими обсягами даних, аби постачальники послуг могли займатися найважливішими в першу чергу. Визначати пріоритетність найкраще узгоджено в усіх правоохоронних органах на загальнодержавному й, по змозі, міжнародному рівні.

31. Доцільність запитів – Правоохоронні органи слід заохочувати не забувати про витрати, які постачальники послуг несуть у зв'язку із запитами, і надавати постачальникам послуг достатньо часу для реагування. Вони мають пам'ятати про те, що постачальники послуг, можливо, мусять реагувати на запити інших правоохоронних органів, і ретельно відслідковувати обсяги, що представляються.

32. Конфіденційність даних – Правоохоронним органам слід гарантувати конфіденційність одержуваних даних.

33. Уникати зайвих витрат і порушення ділових операцій – Правоохоронним органам слід рекомендувати діяти так, щоб уникати зайвих витрат і порушення ділових операцій постачальників послуг і інших суб'єктів господарської діяльності.

34. Правоохоронним органам слід рекомендувати обмежити використання служби контактних пунктів (осіб) в надзвичайних ситуаціях тільки вкрай терміновими випадками, аби не зловживати такою послугою.

35. Правоохоронні органи слід заохочувати своєчасно видавати постанови про розголошення інформації після постанов про збереження чи інші проміжні заходи, або своєчасно повідомляти постачальника послуг мережі Інтернет про те, що необхідність в подальшому зберіганні даних зникла.

36. Міжнародні запити – У разі спрямування запитів іноземним постачальникам послуг мережі Інтернет, національні правоохоронні органи слід заохочувати направляти запити таким постачальникам послуг мережі Інтернет не безпосередньо, а з використанням процедур, описаних у міжнародних угодах, таких як Конвенція про кіберзлочинність, а також в разі термінових заходів, включаючи постанови про збереження / запити, через цілодобову мережу (пунктів) контактів правоохоронних органів.

37. Запити про міжнародну взаємну правову допомогу – Правоохоронні органи і органи кримінальної юстиції слід заохочувати до вживання необхідних заходів, щоб забезпечити, що після запитів про застосування запобіжних заходів, використовуються міжнародні процедури у сфері взаємної правової допомоги, або що постачальники послуг мережі Інтернет вчасно повідомлені про те, що потреба в збереженні даних зникла.

38. Координація між правоохоронними органами – правоохоронні органи слід заохочувати до координування їхньої співпраці з постачальниками послуг мережі Інтернет і взаємного обміну передовою практикою як на національному, так і міжнародному рівні. На міжнародному рівні їм із цією метою слід використовувати відповідні міжнародні представництва.

39. Програми контролю дотримання кримінально-правових норм – Правоохоронні органи слід заохочувати до організації окреслених вище форм взаємодії з постачальниками послуг у вигляді комплексної програми контролю дотримання кримінально-правових норм, і до надання постачальникам послуг опису такої програми, включаючи:

- інформацію, необхідну для встановлення зв'язку з визначеним персоналом правоохоронних органів, відповідальним за програму контролю дотримання кримінально-правових норм, а також про режим роботи такого персоналу

- інформацію, необхідну для того, щоб постачальник послуг міг надавати документи персоналові, відповідальному за контроль дотримання кримінально-правових норм

- інші подробиці, що мають відношення до правоохоронців, відповідальних за контроль дотримання кримінально-правових норм (наприклад, обсяг співробітництва правоохоронних органів з іншими країнами, документи, що підлягають перекладові певною мовою тощо).

40. Аудит системи контролю дотримання – Правоохоронні органи слід заохочувати до відстеження й перевірки системи обробки запитів із статистичною метою, у тому числі з метою визначення її сильних і слабких сторін і, за потреби, публікувати результати таких дій.

Заходи, яких слід уживати постачальниками послуг

41. Співробітництво з метою мінімізації використання послуг з неправомірною метою – За умови дотримання застосовних прав і свобод, таких як свобода вираження поглядів, таємниця особистого життя й інших норм внутрішньодержавного або міжнародного права, а також умов угод з користувачами, постачальників послуг слід заохочувати до співробітництва з правоохоронними органами з метою зведення до мінімуму можливості використання послуг у злочинній діяльності згідно з визначенням закону.

42. Постачальників послуг слід заохочувати до повідомлення правоохоронних органів про ті випадки з кримінально-правовими наслідками, що зачіпають постачальника послуг мережі Інтернет, про які йому стало відомо. Це не зобов'язує постачальників послуг вживати активних заходів для виявлення фактів або обставин, що вказують на такі протизаконні дії.

43. Постачальникам послуг слід рекомендувати сприяти правоохоронним органам в заходах освіти, навчання та надавати інші форми підтримки в зв'язку з їхніми послугами й діяльністю.

44. Реагування на запити правоохоронних органів – Постачальникам послуг слід рекомендувати докладати всіх обґрунтованих зусиль для сприяння правоохоронним органам у виконанні запитів.

45. Порядок реагування на запити – Постачальників послуг слід заохочувати до розробки письмових процедур обробки запитів, включаючи відповідні заходи належної обачності, і до забезпечення відповідності реагування на запити погодженим процедурам.

46. Навчання – Постачальникам послуг слід рекомендувати забезпечити навчання персоналу, відповідального за здійснення цих процедур, в достатньому обсязі.

47. Призначення контактних осіб - Постачальникам послуг слід рекомендувати призначити кваліфікований (підготовлений) персонал в якості контактних осіб для співробітництва із правоохоронними органами.

48. Допомога в надзвичайних ситуаціях – Постачальникам послуг слід рекомендувати передбачити засіб, що дозволяв би правоохоронним органам зв'язуватися з їхніми співробітниками, відповідальними за контроль дотримання кримінально-правових норм, поза звичайним робочим часом з метою реагування на надзвичайні ситуації. Постачальникам послуг слід рекомендувати повідомити правоохоронним органам відповідну інформацію для надання допомоги в надзвичайних ситуаціях.

49. Ресурси – Постачальникам послуг слід рекомендувати забезпечити своїх контактних осіб або персонал, відповідальний за співробітництво із правоохоронними органами, тими ресурсами, які їм необхідні для виконання запитів з правоохоронних органів.

50. Програми контролю дотримання кримінально-правових норм – Постачальникам послуг слід рекомендувати організувати їхнє співробітництво з правоохоронними органами у формі комплексних програм контролю дотримання кримінально-правових норм, і надати правоохоронним органам опис таких програм, включаючи:

- інформацію, необхідну для здійснення зв'язку із призначеним персоналом постачальників, відповідальним за контроль дотримання кримінально-правових норм, а також режим роботи такого персоналу;

- інформацію, необхідну для того, щоб правоохоронні органи могли надати документи персоналові, відповідальному за контроль дотримання кримінально-правових норм;

- інші докладні відомості, що мають стосунок до персоналу постачальників, відповідальному за контроль дотримання кримінально-правових норм (обсяг діяльності постачальника послуг в інших країнах, документи, що підлягають перекладу певною мовою тощо.);

- з метою забезпечити правоохоронним органам можливість спрямування конкретних і доречних запитів, постачальникам послуг слід рекомендувати надавати інформацію про тип послуг, пропонованих користувачам, включаючи гіперпосилання на послуги у всесвітній мережі Інтернет і додаткові відомості, а також контактну адресу для одержання додаткової інформації;

- у тих випадках, коли це можливо, постачальникові послуг мережі Інтернет слід рекомендувати надавати на запит перелік категорій даних, які могли б надаватися правоохоронним органам щодо кожної послуги в разі одержання дійсного запиту правоохоронних органів про розкриття інформації, при цьому слід розуміти, що не всі такі дані є в розпорядженні при проведенні кожного карного розслідування.

51. Перевірка джерела запитів – Постачальникам послуг слід рекомендувати ужити заходів для здійснення перевірки справжності запитів, одержуваних від правоохоронних органів, у межах їхніх можливостей і в міру необхідності, з метою запобігання розголошення облікових матеріалів про їхніх клієнтів неуповноваженим особам.

52. Відповідь – Постачальникам послуг слід рекомендувати направляти відповіді на запити правоохоронних органів в письмовій формі (або в іншій юридично прийнятній електронній формі) та забезпечувати наявність документального сліду щодо таких запитів і відповідей, при цьому слід розуміти, що даний слід може й не включати персональні дані.

53. Стандартна форма відповіді – Беручи до уваги форму запитів, використовувану правоохоронними органами, постачальникам послуг слід рекомендувати стандартизувати форму спрямування інформації правоохоронним органам.

54. Постачальникам послуг слід рекомендувати обробляти запити вчасно і відповідно до визначених ними письмових процедур, та надавати правоохоронним органам інформацію щодо середнього часу затримки, пов'язаного з надсиланням відповіді на запити.

55. Підтвердження інформації, що надсилається – Постачальникам послуг слід рекомендувати забезпечити повноту, точність і захищеність інформації, що спрямовується правоохоронним органам.

56. Конфіденційність запитів – Постачальникам послуг слід гарантувати конфіденційність одержуваних запитів.

57. Роз'яснення щодо ненаданої інформації – Постачальникам послуг слід рекомендувати представляти запитуючому правоохоронному органу роз'яснення у разі відхилення запитів або неможливості надання інформації.

58. Перевірка системи обробки запитів – Постачальникам послуг слід рекомендувати відстежувати й перевіряти систему обробки запитів зі статистичною метою, аби визначати її сильні й слабкі сторони, та в відповідних випадках публікувати отримані результати.

59. Координація між постачальниками послуг – За умови дотримання антимонопольних норм/ правил конкуренції постачальникам послуг слід рекомендувати координувати своє співробітництво з правоохоронними органами, здійснювати взаємний обмін передовою практикою і використовувати із цією метою професійні об'єднання постачальників послуг.