

УДК 338.46:002+341.48

СКУЛИШ Є.Д., доктор юридичних наук, професор,
Заслужений юрист України,
головний науковий співробітник НДІП НАПрН України

МІЖНАРОДНО-ПРАВОВЕ СПІВРОБІТНИЦТВО У СФЕРІ ПОДОЛАННЯ КІБЕРЗЛОЧИННОСТІ

***Анотація.** Проаналізовано сучасний стан розвитку та прояви кіберзлочинності. Визначені ключові аспекти міжнародного співробітництва у сфері боротьби із кіберзлочинністю. Виявлені основні проблеми міжнародного співробітництва в цій сфері.*

***Ключові слова:** кіберзлочинність, кібертероризм, кібершахрайство, міжнародне співробітництво.*

***Аннотация.** Проанализировано современное состояние развития и проявления киберпреступности. Определены ключевые аспекты международного сотрудничества в сфере борьбы с киберпреступностью. Выявлены основные проблемы международного сотрудничества в этой сфере.*

***Ключевые слова:** киберпреступность, кибертерроризм, кибермошенничество, международное сотрудничество.*

***Summary.** The current condition of development and aspects of computer crime were analyzed. The key aspects of international cooperation in the field of the computer crime's combating were determined. The basic problems of international cooperation in this sphere were identified.*

***Keywords:** computer crime, cyberterrorism, cyberswindle, international cooperation.*

***Актуальність теми.** Сучасний стан розвитку телекомунікаційних, інформаційних та комп'ютерних технологій обумовлює появу та швидкий розвиток суспільних відносин з приводу їх використання. Це вимагає їх правову регламентацію, яка відповідала б інтересам суб'єктів таких відносин та економічній доцільності використання предметів, що уособлюють в собі подібні технології. Більше того, інформаційні технології та комп'ютерні мережі на сьогодні являють собою важливу галузь економіки, розвиток якої виходить за межі економіки однієї країни і характеризується наявністю усталених міжнародних зв'язків. Однак технології такого рівня розвитку дедалі частіше використовуються не в економічній площині, а в злочинних інтересах. Зокрема, існує тенденція до перенесення корисливих злочинів у сфері протиправного заволодіння платіжними засобами у віртуальну реальність. Це пояснюється зростанням електронних платежів, що стало можливими саме завдяки розвитку та поширенню використання інформаційних технологій та комп'ютерних мереж. В цьому контексті ключовим стає питання міжнародного співробітництва в сфері захисту інформації та мереж. Взаємодія різних держав та різних компаній є можливою лише за умови створення та функціонування посередників, що мають відповідний міжнародно-правовий статус, оскільки національне законодавство країн-учасників економічних відносин предметом яких є комп'ютерні та інформаційні технології, є неоднорідним, що ускладнює отримання необхідного правозахисного ефекту. Разом з тим, все актуальніше звучить питання стосовно розробки єдиного правового поля, в рамках якого відбуватиметься захист від злочинів, що скоюються у сфері використання комп'ютерних технологій.*

Ступінь наукової розробки теми. Проблематика розробки ефективних правових механізмів міжнародної боротьби із кіберзлочинністю знайшла своє відображення в працях багатьох вітчизняних і закордонних вчених, зокрема О.С. Алавердова, Ю.М. Батуріна, П.Д. Біленчука, А.В. Войцехівського, В.Б. Вехової, В.О. Голубєва, М.Д. Діхтяренка, Т.Л. Тропіної, Б.Х. Толеубєкова та ін.

Метою статті є вдосконалення міжнародної боротьби із кіберзлочинністю в аспекті підвищення ефективності міжнародної співпраці.

Виклад основних положень. Не зважаючи на досить недавню появу, кіберзлочинність перетворилася із протиправної поведінки на одну із найбільших цивілізаційних загроз. З кожним роком феномен кіберзлочинності набирає обертів і стає дедалі поширенішим видом злочинів, що обумовило необхідність розробки відповідного теоретико-методологічного апарату юридичної науки, і зокрема кримінально-правової науки. Однак і досі немає одностайності у визначенні поняття “кіберзлочинність”, що призводить до суттєвих проблем у сфері міжнародного співробітництва, і насамперед у правовій площині.

Російський вчений В.О. Голубєв визначає кіберзлочинність як протиправну поведінку, спрямовану на порушення суспільних відносин та персональної або корпоративної безпеки під час здійснення особами обміну даних за допомогою електронних засобів [4]. М.С. Дашян зазначає, що комп’ютерна злочинність – це порушення чужих прав та інтересів по відношенню до автоматизованих систем обробки даних [6]. А.В. Юрасов вказує, що поняття “кіберзлочинність” охоплює комп’ютерну злочинність (де комп’ютер – предмет злочину, а інформаційна безпека – об’єкт злочину) та інші зазіхання, де комп’ютер є знаряддям або способом вчинення злочину проти власності, майнових та немайнових прав, громадської безпеки тощо [9]. П.Д. Біленчук під кіберзлочинністю розуміє злочини у сфері використання комп’ютерних та інформаційних мереж, наслідком яких є протиправне заволодіння даними [3]. Власне це визначення найбільш наближене до офіційної української кримінально-правової доктрини, оформленої у Кримінальному кодексі України.

Отже, кіберзлочинність як явище виникло виключно в процесі еволюції комп’ютерних та інформаційних технологій, а метою злочинців є персональні та корпоративні дані, які самі по собі становлять цінність або за допомогою яких злочинці протиправним шляхом можуть заволодіти грошима, нематеріальними активами або майновими чи немайновими правами тощо. На сьогодні існує багато типів кіберзлочинів, серед яких найбільшу загрозу представляють: он-лайн шахрайство, DoS-атаки, дефейс, розповсюдження шкідливих програм (вірусів), кардерство, фішинг, комп’ютерне шпигунство, екстремізм у мережі (який все частіше кваліфікується як кібертероризм), особиста образа або наклеп тощо. Більшість із перелічених вище злочинів скоюються не лише на території або у віртуальному просторі однієї конкретної країни, вони можуть мати і більш глобальний міждержавний чи навіть міжнародний характер. Власне це і породжує потребу міжнародного співробітництва, оскільки одна з основних проблем, з якою стикаються оперативні співробітники правоохоронних органів під час розслідування кіберзлочинів, – це складність у встановленні особи злочинця, його державно-територіального місцезнаходження, а також норми права, згідно з якою злочинець може бути притягнутий до відповідальності.

Узагальнюючи викладене вище, можна зробити висновок, що поява та подальший розвиток міжнародного співробітництва у сфері боротьби з кіберзлочинністю має на меті вирішення трьох завдань: персоналізація особи злочинця, визначення юрисдикції та

головне – вибір найбільш адекватного правового впливу на злочинця з метою обов’язкового притягнення його до відповідальності за скоєння такого злочину.

Всі міжнародні організації відзначають необхідність скоординованої міждержавної взаємодії при розслідуванні кіберзлочинів. Саме завдяки роботі таких міжнародних організацій, як Організація економічного співробітництва і розвитку (далі – ОЕСР), Інтерпол, Група Восьми (далі – G8), Рада Європи, ООН, розвивається міжнародна співпраця країн у сфері боротьби з кіберзлочинністю, формується міжнародне законодавство. Проте для розробки і впровадження міжнародно-правових норм необхідний єдиний підхід до розуміння поставлених проблем, визначення єдиних завдань, вироблення загальних принципів. Неузгоджений підхід у кримінальному законодавстві різних держав до формулювання конкретних складів злочинів не сприяє ефективній протидії комп’ютерним злочинам у глобальному масштабі. У зв’язку з цим міжнародно-правове регулювання повинне відігравати головну роль в гармонізації національного кримінального законодавства з міжнародно-правовими актами, розробленими і прийнятими відповідними організаціями [2].

Розглядаючи генезу міжнародно-правової співпраці в області протидії кіберзлочинності в новітній історії, відзначимо, що вже в квітні 1995 р. було проведено I Міжнародну конференцію Інтерполу з комп’ютерної злочинності. У 1996 році країнами G8 було прийнято рішення про створення спеціальної підгрупи по боротьбі з міжнародними злочинами у сфері високих технологій – “Ліонська група”. В цей же час глави країн схвалили прийняття плану з протидії кіберзлочинності. З найбільш важливих пунктів документа варто відзначити: створення в кожній країні контактного центру, що працює 24 години на добу, для співпраці в боротьбі з інформаційними злочинами, надання допомоги кваліфікованими співробітниками правоохоронних органів іншим державам, розробку і використання сумісних стандартів для отримання і перевірки достовірності електронних даних у ході судового розслідування, ознайомлення із законодавчими методами боротьби з комп’ютерними правопорушеннями країн-учасниць. У 2000 р. на Десятому конгресі із запобігання злочинності і поводження з правопорушниками, що проводився в рамках ООН наголошувалося на продовженні зростання світової кіберзлочинності, появі нових видів злочинів у сфері високих технологій і, разом з тим, на нездатності держав і організацій впоратися з кількістю проблем правового характеру, що збільшується, як у рамках національного, так і міжнародного права. У березні 2001 р. Комісія із запобігання злочинності і кримінального правосуддя ООН представила спеціальну доповідь, в якій була вперше наведена класифікація кіберзлочинів [2].

Не менш важливим документом у рамках ООН є Резолюція “По боротьбі із злочинним використанням інформаційних технологій” від 2001 року. У ній наголошується на необхідності співпраці між державами і приватним сектором у боротьбі із злочинним використанням інформаційних технологій, яка повинна досягатися шляхом: введення в законодавство відповідальності за інформаційні злочини; транснаціональної співпраці правоохоронних органів; міжнародного обміну інформацією про проблеми злочинного використання інформаційних технологій; навчання співробітників правоохоронних органів в умовах інформаційного суспільства; захисту комп’ютерних систем від несанкціонованого втручання тощо. Окремо слід відзначити п 1. Резолюції, в якому вказано, що інформаційні технології повинні розроблятися так, щоб сприяти запобіганню і виявленню випадків злочинного використання, відстежуванню злочинців і збору доказів. Теоретично даний пункт надає правоохоронним органам окремої країни можливість здійснювати виявлення і

організовувати заходи із затримання злочинців у короткий строк і з більшою ефективністю. Але існує можливість неправомірного доступу злочинців до вищезгаданих технологій і використання прихованих можливостей систем з метою скоєння інформаційних злочинів, наприклад, розкрадання персональних даних. В рамках співпраці держав-учасників СНД в 2001 році було укладено Угоду по боротьбі із злочинами у сфері комп'ютерної інформації, відповідно до якої сторони здійснюють співпрацю у формах обміну інформацією, проведення розслідувань у сфері комп'ютерної інформації, сприяння в підготовці кадрів, проведення спільних наукових досліджень, створення інформаційних систем, обміну нормативно-правовими актами і науково-технічною літературою з боротьби із комп'ютерними злочинами [7].

На сьогодні основним документом, який регулює питання міжнародної співпраці у сфері запобігання та протидії кіберзлочинності є Конвенція про кіберзлочинність (далі – Конвенція), яка була підписана 23 листопада 2001 р. в Будапешті. В цій Конвенції сформульовано найбільш загальні та разом із тим визначальні принципи щодо забезпечення заходів боротьби із кіберзлочинами на національному та міжнародному рівнях. Відповідно до ст. 23 сторони співпрацюють між собою у найширших обсягах шляхом застосування відповідних міжнародних документів щодо міжнародного співробітництва у кримінальних питаннях, угод, укладених на основі єдиного чи взаємного законодавства, і внутрішньодержавного законодавства з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, які стосуються кримінальних правопорушень.

Конвенція виділяє чотири групи правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем:

- злочини у сфері незаконного доступу до інформації: нелегальне перехоплення (ст. 3), втручання у дані (ст. 4), втручання у систему (ст. 5), зловживання пристроями (ст. 6);
- злочини, пов'язані з протиправним використанням комп'ютерів: підробка, пов'язана з комп'ютерами (ст. 7), шахрайство, пов'язане з комп'ютерами (ст. 8);
- злочини, пов'язані зі змістом, до яких відноситься створення, розповсюдження та зберігання дитячої порнографії (ст. 9);
- злочини, пов'язані з порушенням авторських та суміжних прав (ст. 10) [1].

В цьому контексті виникає одна з перших проблем міжнародного співробітництва, оскільки акценти правового впливу, розставлені в Конвенції, не відповідають реальним сучасним умовам розвитку кіберзлочинності: на перше місце виходить не просто кіберзлочинність, а її крайній прояв – кібертероризм. У зв'язку з цим науковцями була розроблена класифікація джерел кіберзлочинів з метою якнайшвидшої ідентифікації загрози та вжиття необхідних заходів по її усуненню. З огляду на це фахівці поділяють осіб і організації, що здійснюють атаки, на декілька категорій, відповідно до яких і формуються категорії самих кіберзлочинів [8]:

хакери – особи, що мають високий рівень знань в області комп'ютерних технологій і проводять багато часу за комп'ютером у пошуках слабких місць комп'ютерних систем (для них притаманне скоєння таких злочинів, як DoS-атаки, дефейс, розповсюдження шкідливих програм (вірусів), фішинг);

хактивісти, чия діяльність є своєрідним синтезом соціальної активності, ставлячи за мету протест проти чого-небудь, і хакерства (використання Інтернет-технологій з метою спричинення збитку комп'ютерним мережам і їх користувачам). Для них притаманне скоєння таких злочинів, як розповсюдження шкідливих програм (вірусів), особиста образа або наклеп;

власне кіберзлочинці, чия діяльність спрямована на незаконне отримання прибутків (для них притаманне скоєння таких злочинів, як кардерство, фішинг, кібершахрайство тощо);

особи, що професійно займаються промисловим шпигунством;

кібертерористи, чия діяльність пов'язана із різного роду екстремістськими проявами в мережі. На сьогодні терористи досягли того рівня, за якого вони можуть використовувати Інтернет (як сам по собі, так і у поєднанні з фізичною атакою) як інструмент для спричинення реальної шкоди.

Важливим аспектом, на якому акцентується увага при вивченні Конвенції, є той факт, що в ній приділяється окрема увага співучасті у скоєнні кіберзлочинів, при чому виділяється відповідальність за спробу і допомогу (ст. 11) та корпоративна відповідальність (ст. 12). Що ж стосується санкцій за скоєння даних правопорушень, то у ст. 13 зазначається, що кожна країна, яка ратифікувала Конвенцію, вживає такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення того, щоб кримінальні правопорушення, встановлені відповідно до статей 2-11, каралися ефективними, пропорційними і переконливими санкціями, включаючи позбавлення волі. Також відзначається необхідність забезпечення відповідальності юридичних осіб на принципах ефективних, пропорційних і переконливих кримінальних або некримінальних санкцій чи заходів, включаючи грошові санкції.

Відповідно до ст. 15 Конвенції кожна країна, що її ратифікувала, забезпечує, щоб встановлення, імплементація і застосування повноважень і процедур, передбачених Конвенцією, регулювалися умовами і запобіжними заходами, регламентованими внутрішньодержавним правом, які забезпечували б адекватний захист прав і свобод людини. Конвенція передбачає такі види запобіжних заходів [1]:

– заходи загального характеру, до яких відносяться термінове збереження комп'ютерних даних, які зберігаються (ст. 16), та термінове збереження і часткове розкриття даних про рух інформації (ст. 17);

– заходи представлення (ст. 18), які регламентують порядок та межі видачі відповідних ордерів для здійснення необхідних процесуальних дій на національній території правоохоронним органам інших країн;

– обшук і арешт комп'ютерних даних, які зберігаються (ст. 19);

– збирання комп'ютерних даних у реальному масштабі часу, до яких відносяться збирання даних про рух інформації у реальному масштабі часу (ст. 20) та перехоплення даних змісту інформації (ст. 21).

Що ж стосується процесу міжнародного співробітництва у сфері безпосередньої боротьби (оперативна діяльність правоохоронних органів) з кіберзлочинцями, то Конвенція застосовує, зокрема, такі заходи [1]:

– екстрадиція (ст. 24);

– взаємна допомога (ст. 25), коли сторони надають одна одній взаємну допомогу в найширшому обсязі з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі щодо кримінального правопорушення;

– добровільна допомога (ст. 26), коли сторона може в рамках свого законодавства без попереднього запиту надіслати іншій стороні інформацію, отриману в ході її власного розслідування, якщо вона вважає, що розкриття такої інформації може допомогти стороні, яка отримує інформацію, у відкритті або проведенні розслідування чи переслідуванні стосовно кіберзлочинів;

– взаємна допомога щодо тимчасових заходів, яка включає термінове збереження комп’ютерних даних, які зберігаються (ст. 29), та термінове розкриття збережених даних про рух інформації (ст. 30);

– взаємна допомога щодо повноважень на розслідування, а саме: взаємна допомога щодо доступу до комп’ютерних даних, які зберігаються (ст. 31); транскордонний доступ до комп’ютерних даних, які зберігаються, за згодою або у випадку, коли вони є публічно доступними (ст. 32); взаємна допомога у збиранні даних про рух інформації у реальному масштабі часу (ст. 303); взаємна допомога у перехопленні даних змісту інформації (ст. 34);

– цілодобова мережа, тобто створення та підтримання в актуальному стані мережі в рамках якої відбувається обмін інформацією різного роду щодо запобігання кіберзлочинам (ст. 35).

Розглядаючи проблеми боротьби з кіберзлочинністю, через призму Конвенції можна дійти висновку щодо вироблення загальної позиції з питання про те, які діяння, пов’язані з використанням комп’ютерних систем, мають бути криміналізовані.

По-перше, такі дії вважаються злочинними і допускають застосування сили, необхідної для ефективної боротьби з ними, а також заходів, необхідних для виявлення, розслідування і судового переслідування таких злочинів як усередині держави, так і на міжнародному рівні.

По-друге, наявність в Конвенції статті “Пошук і конфіскація збережених комп’ютерних даних” дає можливість одній стороні добитися збереження важливої інформації, необхідної для розслідування злочину, яка знаходиться в юрисдикції іншої сторони. Наскільки відомо, провайдер послуг Інтернету, як правило, має в своєму розпорядженні дані про інформаційний обмін повідомленнями у минулому, що можна отримати за допомогою устаткування, яке реєструє конкретні аспекти інформаційного обміну, включаючи час, тривалість і дату будь-якого повідомлення. Такі дані зберігаються зазвичай протягом обмеженого періоду часу, залежного від комерційних потреб оператора або постачальника послуг, а також юридичних вимог, що стосуються нерозголошення приватної інформації. Національне законодавство багатьох країн дозволяє правоохоронним або судовим органам видавати розпорядження, що стосується збору даних інформаційного обміну. Важливим є положення Конвенції, яке дає можливість приймати законодавчі й інші заходи, що уповноважують компетентні органи конфіскувати або так само захистити від знищення дані, які є у провайдера і необхідні для розслідування.

Безперечно, з правової точки зору велике значення мають і загальні принципи, що стосуються міжнародної співпраці, які визначені в Конвенції. Це питання видачі комп’ютерних злочинців і надання країнами одна одній широкої взаємодопомоги для розслідування кримінальних справ, пов’язаних з комп’ютерними системами і даними, так само як і для збору електронних доказів. З урахуванням специфіки соціального феномена кіберзлочинності, масштабів інформатизації і розвитку глобальної мережі Інтернет стає все менш вірогідним, що злочини такого роду будуть обмежені територією окремої держави. У процесі проведення розслідувань правоохоронні органи різних держав повинні співпрацювати між собою, причому як офіційно, використовуючи такі рамки і структури як, наприклад, Інтерпол та ін., так і неофіційно, надаючи потенційно корисну інформацію безпосередньо правоохоронним органам іншої держави. У зв’язку з правовою допомогою при розслідуванні кіберзлочинів неминуче виникатимуть і інші додаткові проблеми. Якщо внутрішнім правом однієї країни не передбачені конкретні повноваження на пошук доказів в інформаційній мережі, то така сторона не буде здатна

адекватно реагувати на запит про надання допомоги від іншої сторони. В цьому аспекті важливою умовою міжнародного співробітництва є узгодження повноважень щодо вжиття необхідних заходів для розслідування кіберзлочинів [5].

Слід відзначити, що в ряді країн Західної Європи діє правова доктрина, згідно з якою держава може застосовувати свою юрисдикцію на території іншої країни у випадку, якщо протиправні посягання торкнулися інтересів даної держави. Проте Європейський Союз звертає увагу, що дане положення потребує міжнародного врегулювання, оскільки держави деколи надмірно широко тлумачать норми даної доктрини. На сьогодні пріоритетним завданням міжнародної взаємодії є уніфікація національного кримінального законодавства країн, що беруть участь в процесі міжнародного співробітництва у сфері боротьби із кіберзлочинністю, навіть незважаючи на наявність Конвенції [7].

Тенденція зростання кіберзлочинності і тенденція “відставання” соціально-правового контролю над нею утворюють надзвичайно велику цивілізаційну загрозу, подолати яку можна лише шляхом органічного поєднання кримінально-правових і криміналістичних стратегій боротьби з цим видом злочинів. Причому важливою складовою такої стратегії повинна стати більш прозора та оперативна міжнародна співпраця в цій сфері, оскільки вже очевидно, що контролювати транснаціональну складову кіберзлочинності та кібертероризму на рівні окремих держав неможливо. Власне цей комплекс проблем і має невідкладно вирішувати міжнародне співтовариство в XXI столітті.

Висновки.

Поява та подальший розвиток міжнародного співробітництва у сфері боротьби з кіберзлочинністю має на меті вирішення трьох завдань: персоналізація особи злочинця, визначення юрисдикції та, головне, – вибір найбільш адекватного правового впливу на злочинця з метою обов’язкового притягнення його до відповідальності за скоєння такого злочину.

Стан міжнародного співробітництва у сфері боротьби з кіберзлочинністю на сьогодні не є однозначним. З одного боку, кількість країн-учасниць такого співробітництва дозволяє охопити та контролювати більше 80 % відносин у сфері інформаційних та комп’ютерних технологій. З іншого ж, ефективність міжнародно-правових засобів боротьби залишається низькою.

В першу чергу це пояснюється об’єктивними причинами, зокрема невідповідністю інтенсивності появи способів вчинення кіберзлочинів та оперативності правового реагування міжнародної спільноти.

По-друге, існує проблема узгодженості дій країн-учасниць Конвенції та швидкості їх спільних дій, вирішення якої лежить в площині взаємної відкритості національних законодавств. Більше того, взаємодія країн з приводу боротьби з кіберзлочинами обумовлює необхідність взаємного проникнення правоохоронних структур ув сферу суспільних відносин з приводу інформації, що часто становить комерційну таємницю чи містить обмежені для користування персональні дані. Іншими словами, вважається, що пошук шляхів підвищення ефективності боротьби з кіберзлочинами лежить в площині вирішення суперечностей у сфері правового регулювання інформаційного простору та створення єдиних правил його використання як в приватних, так і в корпоративних інтересах.

Використана література

1. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.01 р. – Режим доступу : [//www.zakon2.rada.gov.ua/laws/show/994_575](http://www.zakon2.rada.gov.ua/laws/show/994_575)

2. Алавердов О.С. Международное сотрудничество в области борьбы с Интернет-преступностью / О.С. Алавердов // Общество и право. – 2010. – № 3.
3. Біленчук Д.П. Кібрешахраї – хто вони? // Міліція України. – 1999. – № 7-8. – С. 32-34.
4. Голубев В.А. “Кибертерроризм” – миф или реальность? / В.А. Голубев. – Режим доступа : //www.crime-research.org. – (Computer Crime Research Center – Центр исследования компьютерной преступности).
5. Голубев В.А. Электронный терроризм – проблемы противодействия // Компьютерная преступность и кибертерроризм. Исследования, аналитика. – Вып. 2. – Запорожье, 2004. – С. 13-17.
6. Дашян М.С. Право информационных магистралей. – М. : Норма, 2007. – 288 с.
7. Кривогин М.С. Международно-правовые аспекты борьбы с кибернетическими преступлениями : материалы II междунар. науч. конф. [“Государство и право : теория и практика”], (Чита, март 2013 г.). – Чита : Издательство “Молодой ученый”, 2013. – С. 77-79.
8. Тропина Т.Л. Киберпреступность : понятие, состояние, уголовно-правовые меры борьбы / Т.Л. Тропина. – Владивосток, 2007.
9. Юрасов А.В. Основы электронной коммерции : учебник / А.В. Юрасов. – М. : Горячая линия-Телеком, 2008. – 480 с.

~~~~~ \* \* \* ~~~~~