МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

# ОСОБЛИВОСТІ ВИЯВЛЕННЯ ФАКТІВ, ПОВ'ЯЗАНИХ ІЗ НЕЗАКОННИМ РОЗПОВСЮДЖЕННЯМ МЕДІЙНОГО КОНТЕНТУ В МЕРЕЖАХ ПРОВАЙДЕРІВ ПРОГРАМНОЇ ПОСЛУГИ ТА ІНТЕРНЕТ-ПРОВАЙДЕРІВ, МЕРЕЖІ ІНТЕРНЕТ

*Методичні рекомендації*

**Дніпро 2017**

**ББК 67.9(4УКР)312**
**О-75**

*Рекомендовано*
*Науково-методичною радою*
*Дніпропетровського державного*
*університету внутрішніх справ*
*(протокол № 7 від 23.03. 2017 р.)*

**Авторський колектив:** *Гавриш О.С.* – викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ; *Краснобрижий І.В.* – старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, к.ю.н.; *Мирошниченко В.О.* – викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, к.т.н., доцент; *Прокопов С.О.* – старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ; *Рижков Е.В.* – завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, к.ю.н., доцент.

**Рецензенти:**

**Ісмайлов Карен Юрійович** – завідувач кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ, кандидат юридичних наук, майор поліції;

**Санакоев Дмитро Борисович** – доцент кафедри оперативно-розшукової діяльності та спеціальної техніки Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, доцент, підполковник поліції.

**О-75** Особливості виявлення фактів, пов’язаних із незаконним розповсюдженням медійного контенту в мережах провайдерів програмної послуги та Інтернет-провайдерів, мережі Інтернет: методичні рекомендації / [Гавриш О.С., Краснобрижий І.В., Мирошниченко В.О., Прокопов С.О., Рижков Е.В]. – Дніпро: Дніпроп. держ. ун-т. внутр. справ, 2017. – 44 с.

З урахуванням сучасних потреб правоохоронної практики, стану розвитку інформаційних технологій та кримінально-правової науки розглянуті сучасні тенденції боротьби з незаконним розповсюдженням медійного контенту в мережах провайдерів програмної послуги та Інтернет-провайдерів, мережі Інтернет.

Методичні рекомендації розраховані на працівників підрозділів боротьби із кіберзлочинністю, слідчих, викладачів, курсантів та студентів юридичних вузів, аспірантів, магістрів, а також усіх, хто цікавиться зазначеним питанням.

**Зміст**

## Вступ

Стрімкий та динамічний розвиток інформаційних технологій кожен день все більше змінює аспекти економічного, політичного і соціального життя у всіх країнах світу. Але розширення інформаційного обміну супроводжується не тільки процесами, які збільшують культурно-комунікативні можливості людини, але й такими, що створюють підґрунтя для виникнення нових форм злочинності у сфері високих технологій.

Злочини у сфері сучасних інформаційних технологій набувають міжнародного та транснаціонального характеру, у зв'язку з чим потерпілі від таких злочинів можуть знаходитись в різних країнах світу. Тому для протидії таким видам злочинів особливе значення має посилення й удосконалення міжнародного співробітництва в даній сфері, підвищення його ефективності.

Наразі вказані проблеми мають тенденцію до того, що міжнародні організації та органи влади багатьох країн вживають організаційних та правових заходів щодо запобігання та протидії злочинам у сфері сучасних інформаційних технологій. Для підтримки такої позиції на базі використання системи криміналістичної класифікації способів вчинення правопорушень у сфері інформаційних технологій був розроблений кодифікатор Генерального Секретаріату Інтерполу, де окремо передбачено комп'ютерні злочини. З метою запобігання злочинам, вчиненим у сфері інформаційних технологій, 23 листопада 2001 року в Будапешті було підписано Конвенцію Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185, більш відому в Україні під назвою «Конвенція про кіберзлочинність». Вона відкрита для підписання як державами – членами Ради Європи, так і тими державами, які не є її членами та брали участь в її розробці. Зокрема, її підтримали США і Японія. Крім того, Європейським комітетом з проблем злочинності Ради Європи в 1990 році, з метою підвищення ефективності протидії таким видам злочинів та правового визначення в Європі групи злочинів, пов'язаних з комп'ютерами й інформаційними технологіями, було підготовлено рекомендації про включення в законодавство європейських країн кримінальних норм «мінімального списку» і «необов'язкового списку» комп'ютерних злочинів.

## 1. Міжнародний досвід регулювання всесвітньої мережі Інтернет. Варіанти розміщення систем технічної фільтрації

*Регулювання Інтернету в Великобританії*

Підхід до фільтрації контенту у Великобританії являє собою особливий інтерес у зв'язку з тим, що саме британська система регулювання Мережі була взята за зразок при створенні Ліги безпечного Інтернету й ініціюванні закону № 139-ФЗ, у рамках якого з'явився «реєстр заборонених сайтів».

Уряд Великобританії в середині 2000-х років позначив два ключових завдання, які мали переслідувати фільтрацію інтернет-контенту: боротьба з тероризмом і запобігання поширенню дитячої порнографії. Пізніше до цього переліку додалася боротьба із систематичним порушенням авторських прав.

Ключову роль у питаннях регулювання контенту в Мережі грають не державні органи, а благодійний Фонд спостереження за Інтернетом (Internet Watch Foundation), заснований в 1996 році. Фінансування фонду частково забезпечують британські оператори зв’язку, інтернет-компанії й виробники програмного забезпечення, а частково – уряд Великобританії й структури Євросоюзу.

Офіційно завданням, що декларується IWF, є «мінімізація доступності потенційно незаконного інтернет-контенту, особливо дитячої порнографії, незалежно від того, де він розміщений, а також видалення незаконного порнографічного контенту, розміщеного на території Великобританії». Раніше організація ставила своєю метою також боротьбу з розпаленням расової ненависті, однак в 2011 році ця функція була передана поліцейському проекту True Vision, що покликаний акумулювати скарги на злочини, пов'язані з розпаленням ненависті стосовно різних груп населення, і закривати дані ресурси, якщо вони розташовані на британських серверах.

Функція IWF зводиться до ведення реєстру заборонених сайтів, що являє собою набір посилань, переважно пов'язаних із забороненим контентом. Безпосереднім веденням даного реєстру займаються декілька фахівців, навчених поліцією. За різними оцінками, усього в списку IWF одночасно утримується приблизно 1000 функціонуючих сайтів.

У свою чергу, в інтернет-провайдерів встановлено спеціальне програмне забезпечення Cleanfeed, яке покликане блокувати доступ до заборонених сайтів. Дана система була розроблена державною корпорацією British Telecom в 2004 р., і сьогодні її використання є обов'язковим для всіх провайдерів Великобританії, незалежно від того, державні вони чи недержавні. У результаті дія системи Cleanfeed поширюється практично на всіх британських інтернет-користувачів.

Провайдери самі визначають, повідомляти чи ні своїм користувачам про те, що сайт, на який вони хотіли перейти, заблокований Cleanfeed. Деякі виводять відповідне повідомлення, однак більша частина повідомляє про те, що дана сторінка відсутня на сервері (page not found). Таким чином, користувачі не знають про те, що той або інший контент був заблокований. Оскільки блокування здійснюється не за рішенням суду, а сам оператор реєстру не є

державним, процедура апеляції блокування відбувається за внутрішніми правилами IWF.

З 2011 року система Cleanfeed використовується операторами зв'язку. Британська асоціація кінематографістів через суд змусила провайдерів використовувати систему фільтрації медійного контенту для блокування сервісів обміну неліцензійним контентом, що порушує авторські права. Зокрема, у травні 2012 року серед інших блокуванню піддався найбільший торрент-трекер The Pirate Bay.

Технічна реалізація системи виглядає таким чином. Існує конфіденційний список заборонених інтернет-сторінок (не сайтів), доступ до якого мають тільки фахівці IWF. Він не доступний ані провайдерам, ані рядовим користувачам. Провайдерам надається список IP-адрес сайтів, на яких розміщено дані сторінки, для того, щоб саме до цих адрес застосовувалися правила фільтрації.

Провайдери перенаправляють трафік, що йде на ці адреси, на спеціальні проксі-сервери, які порівнюють HTTP-запити з адресами сторінок, що містяться в реєстрі заборонених адрес. Якщо вони не збігаються – трафік проходить фільтр і користувач потрапляє на запитувану сторінку.

Робота Cleanfeed здійснюється у два етапи:

1) перевірка IP-адреси, до якої звернено запит;

2) порівняння сторінки, до якої звертається користувач, зі списком адрес у реєстрі заборонених ресурсів.

Пізніше система Cleanfeed була експортована в деякі країни британської співдружності. У Канаді в цей час вона використовується на добровільній основі найбільшими провайдерами країни, що обслуговують приблизно 80% інтернет-користувачів. В Австралії впровадження даної системи зіткнулося з політичною протидією, тож її реалізація в масштабах країни була відкладена на невизначений термін.

У серпні 2011 року після масових безладів у найбільших британських містах прем'єр-міністр Великобританії Девід Кемерон зустрівся з керівництвом найбільших інтернет-компаній з метою обговорення можливих заходів, які дозволили б запобігти використанню соціальних мереж погромниками. Із цього приводу Кемерон зробив таку заяву в парламенті: «Всі ми вражені тим, що жахливі події, які відбулися в нашій країні, організовані за допомогою соціальних медіа. Вільний потік інформації може використовуватися на благо. Але також він може використовуватися й зі злим наміром. Коли люди використовують соціальні медіа для провокування насильства, наше завдання – зупинити їх. Тому ми працюємо разом з поліцією, розвідувальними службами й інтернет-індустрією над питанням: чи правильно буде призупинити інтернет-комунікацію через певні сайти й сервіси, якщо нам відомо, що за допомогою їх плануються дії, пов'язані зі злочинністю й насильством».

*Регулювання Інтернету в США*

На практику регулювання Інтернету в США великий вплив зробили відразу декілька факторів, зробивши її унікальною серед інших країн. По-перше, США – історична батьківщина Інтернету, а багато американських IT-

компаній, такі як Google, Facebook і Twitter, займають лідируючі позиції в мережі. По-друге, перша поправка Конституції США прямо забороняє приймати закони, що обмежують свободу слова. Отже, багато методів регулювання Інтернету американським законодавцям є недоступними. По-третє, провідна роль США у світовій політиці й економіці дозволяє досягати від іноземних країн і компаній виконання вимог американської влади.

Спроби поставити в обов'язок інтернет-провайдерам і реєстраторам доменів блокувати доступ до сайтів за рішенням суду неодноразово здійснювались правовласниками й прихильниками боротьби із забороненим контентом. Але щораз такі закони не приймалися Конгресом, а рішення судів відмінялися. Так, в 2004 році штат Пенсільванія прийняв закон, що наказував інтернет-провайдерам фільтрувати сайти з дитячою порнографією. Механізм блокування не був добре відпрацьований, і в результаті, крім нелегального контенту, недоступними виявилося більше мільйона інших сайтів. Незабаром федеральний суддя виніс рішення про невідповідність даного закону першій поправці.

В 2012 році Конгрес розглядав проекти законів SOPA і PIPA, які зобов'язували провайдерів і хостерів блокувати доступ до сайтів з матеріалами, що порушують авторські права, за вимогою правовласників. На знак протесту тисячі сайтів, включаючи Вікіпедію й Craigslist, на день перестали працювати. Петиція проти законів, розміщена на сайті Google, зібрала більше 4,5 мільйонів підписів. У результаті розгляд проектів Конгресом було відкладено.

У 2000-х рр. Мін'юст США застосовував тактику з конфіскації доменів сайтів, що порушують закон, трактуючи їх як майно, використовуване для кримінальної діяльності. Цей захід також зазнав критики активістів із захисту свободи слова в Інтернеті. Крім цього його ефективність була сумнівною – найчастіше сайти ставали доступними за новою адресою. Інший випадок блокування DNS-записів державою – застосування Акта про торгівлю з ворогом, що забороняє ведення бізнесу з низкою держав. Відповідно до його положень компанія-реєстратор доменів була змушена блокувати DNS-запис туристичного агентства, що рекламував тури у Кубу.

У цілому сьогодні Інтернет у США залишається вільним від технічних методів цензури з боку держави. Замість цього фільтрація контенту добровільно здійснюється приватними компаніями за підтримки державних структур. Наприклад, у випадку із забороненим контентом ряд великих інтернет-провайдерів підписали угоду з окружним прокурором Нью-Йорка, погодившись добровільно блокувати доступ до таких ресурсів.

Іншим важливим інструментом США з регулювання Інтернету залишається тиск на іноземні компанії. Оскільки в США нелегальною є більшість видів азартних онлайн-ігор, а держава не має можливості блокувати доступ до іноземних сайтів, влада пішла на ряд жорстких заходів щодо порушників. Конгрес прийняв закон, що передбачає заборону онлайн-казино і букмекерським конторам приймати платежі від американських громадян. Google і Yahoo відмовилися від розміщення рекламних банерів таких сайтів, після того як Мін'юст США заявив, що реклама може бути розцінена як

сприяння злочину. Ряд власників букмекерських контор, що працюють онлайн, були піддані карному переслідуванню. Такий тиск дозволяє добиватися від компаній, що перебувають поза юрисдикцією США, виконання вимог американських законів.

США одними з перших прийняли закони, що регулюють інтелектуальну власність в Інтернеті. Відповідно до законодавства, інтернет-провайдери і хостингові компанії звільняються від судової відповідальності за передачу й зберігання інформації, що порушує авторські права, якщо вони видаляють її після звертання правовласника. Закон призвів до того, що, побоюючись позовів, сайти найчастіше видаляють контент за першою вимогою, не вникаючи, чи дійсно він порушує авторські права. Наприклад, Google одержує кілька мільйонів запитів на місяць на видалення посилань з результатів пошуку.

Справжнім тестом для дії першої поправки Конституції США в Інтернеті став скандал навколо сайту Вікілікс. Неприємності з американським правосуддям у нього почалися ще в 2008 році – за позовом швейцарського банку суд наказав заблокувати доменне ім'я сайту. Рішення викликало протести з боку активістських груп і незабаром було скасовано. Справжні ж проблеми викликала публікація в 2010 році засекречених документів і матеріалів, зокрема дипломатичного листування посольств, а також відеозапису розстрілу американськими військовими цивільних осіб в Іраку. Оприлюднення даних матеріалів завдало істотної шкоди національним інтересам США.

Незважаючи на те, що формально публікація третьою стороною незаконно отриманої інформації не суперечить законодавству країни, Міністерство юстиції розглянуло можливість карного переслідування творця сайту Джуліана Ассанджа за обвинуваченням в «крадіжці державної власності» і порушенні Акта про шпигунство від 1917 року. Влада США заблокувала доступ до сайту з комп'ютерів федерального уряду й зробила безпрецедентний тиск на компанії, що працюють із Вікілікс. Зокрема, Amazon відмовився від надання послуг хостингу сайту, а платіжні системи Visa, Mastercard і Paypal перестали приймати платежі на його адресу. Проте переважна більшість інтернет-користувачів США, як і раніше, можуть безперешкодно відвідувати сайт Вікілікс.

*Інтернет-цензура в Ірані*

За часткою населення, що користується Інтернетом, Іран посідає друге місце на Близькому Сході, поступаючись тільки Ізраїлю. У країні особливо розвинена блогосфера – за оцінками експертів, число регулярно обновлюваних блогів перевищує 60000. Зусилля уряду Ірану, з одного боку, спрямовані на розвиток інфраструктури Інтернету, з іншого боку – на повний контроль того, що публікується користувачами в мережі.

В умовах жорстких законів, що регулювали пресу, Інтернет до 2004 року залишався одним з кількох місць, де можна було вільно виражати свою думку. Але поступово таке джерело вільнодумства привернуло увагу влади Ірану, і вона почала реалізацію послідовної політики з боротьби з небажаним контентом. Дію положень закону про пресу було розширено на електронні

публікації. Додатковим стимулом для посилення контролю над Інтернетом стали масові протести після президентських виборів 2009 року, коли опозиція використовувала соціальні мережі для координації акцій і зв'язку із західними агентствами новин.

Обмеження свободи слова прямо передбачено іранською конституцією, в якій сказано, що «засоби масової інформації повинні утримуватися від руйнівних і антиісламських практик». Закон про пресу також обмежує неприпустиму інформацію, зокрема «висвітлення тематик, які шкідливі для основ Ісламської республіки», «образа Лідера Революції», «підбурювання громадян до дій проти безпеки, гідності й інтересів Ісламської республіки». Також заборонені будь-які публікації, що ображають іслам. Такі розпливчасті категорії дозволяють владі блокувати практично будь-яку інформацію зі свого розсуду.

Фільтрація контенту в Інтернеті донедавна здійснювалася на підставі серії постанов Верховної Ради Культурної революції, а визначення критеріїв для блокування було довірено міжвідомчому комітету, в який входять представники міністерств культури, безпеки й генеральної прокуратури. Практичною реалізацією політики фільтрації займається підрозділ головної державної телекомунікаційної компанії й агентство Міністерства по комунікаціях. В 2012 році лідер Ірану Хаменеї оголосив про створення Верховної ради по кіберпростору, що з цього моменту займається створенням єдиної політики стосовно Інтернету.

Всі провайдери країни повинні одержувати ліцензію від державних органів, а користувачі підписують зобов'язання не відвідувати «антиісламські сайти». Для домогосподарств діє ліміт на швидкість в 128 Кбіт/с, що полегшує навантаження на систему фільтрації, а також обмежує доступ користувачів до небажаних західних фільмів і музики. На організації й університети він не поширюється. На даний момент Іран залишається єдиною країною, де діє законодавче обмеження на швидкість доступу в Інтернет для користувачів.

Однією з умов надання провайдерам ліцензії є застосування системи фільтрації, що блокує веб-сторінки за списком, наданим державою. Спочатку вся цензура здійснювалася саме на рівні провайдерів, але в останні роки влада Ірану розробила й впровадила централізовану систему, що працює у зв'язці із фільтрами провайдерів. Цей крок забезпечив більшу однаковість у політиці цезури, тому що раніше вона сильно варіювалася від провайдера до провайдера. Технічна фільтрація в Ірані є прозорою – при спробі звертання до сайту, занесеного в державний список, видається блок-сторінка з роз'ясненням про недоступність ресурсу і контактами адміністратора, якому можна направити запит.

Фільтри, застосовувані в Ірані, являють собою проксі-сервери, на які перенаправляється трафік користувачів. Кожний запит звіряється зі списком заблокованих сайтів і сторінок, а також аналізується на предмет наявності певних ключових слів. У випадку збігу користувач перенаправляється на блок-сторінку.

Ранні дослідження Open Net Initiative показали, що технічним рішенням,

використовуваним інтернет-провайдерами, був SmartFilter американської фірми Secure Computing. Сама компанія-виробник відхиляла продаж програмного забезпечення, стверджуючи, що Іран використовує його незаконно. Співробітництво з Іраном у цій сфері могло стати не тільки серйозним ударом по репутації Secure Computing, але й можливим порушенням економічних санкцій США.

Влада Ірану була незадоволена залежністю своєї системи фільтрації від західних технологій, побоюючись вбудованих «слабких місць», які можуть порушити її роботу. Тому її зусилля були спрямовані на перехід до інформаційних рішень, розроблених місцевими компаніями. Сьогодні технічна система фільтрації Ірану використовує власні розробки не тільки для блокування сайтів, але й для автоматичного пошуку забороненого контенту в мережі.

В Ірані діє тверда система контролю за користувачами. Інтернет-провайдери зобов'язані зберігати протягом трьох місяців не тільки логи, але й саму інформацію, що передається користувачами. Коли один з іранських дисидентів був арештований за висловлення в системі миттєвого обміну повідомленнями, доказом його провини виступила роздруківка його переписки. Користувачі інтернет-кафе повинні надавати свою ідентифікаційну інформацію, а власники зобов'язані встановлювати в приміщенні камери й зберігати записи про відвідувачів.

Думки фахівців розходяться в оцінці здатності Ірану застосовувати технологію глибокого аналізу пакетів. В 2008 році компанію Nokia Siemens Systems обвинуватили в поставках головному телекомунікаційному операторові країни устаткування, яке здатне масово перехоплювати повідомлення користувачів. Однак представник NSS заявив, що його можливості обмежені тільки законним відстеженням комунікацій окремих користувачів у рамках діяльності правоохоронних органів. Розслідування Reuters і Wall Street Journal показало, що дві китайські корпорації Huawei і ZTE співробітничали із владою Ірану в створенні системи інтернет-стеження. Їх представники також відкинули ці обвинувачення. Проте є ряд свідчень того, що Іран має подібну технологію. Так, в 2012 році під час виборів блокувався весь зашифрований трафік.

Правки до закону про пресу Ірану, прийняті в 2009 році, зобов'язують власників сайтів проходити процедуру реєстрації в Міністерстві культури, що має право відзивати ліцензію й забороняти окремі публікації. З положень іншого закону, інтернет-сервіси відповідають за матеріал, розташований у них іншими користувачами. За таких умов широкого поширення набула самоцензура, коли користувачі побоюються висловлювати свою думку онлайн, а власники сайтів зі своєї ініціативи видаляють будь-який спірний контент.

Влада Ірану активно застосовує карне переслідування щодо користувачів Інтернету, у тому числі страту. За інформацією Human Rights Watch, в 2011 р. Іран встановив рекорд за кількістю арештованих блогерів і журналістів. За кримінальним кодексом Ірану покарання аж до страти передбачено за «пропаганду проти держави», «образу релігії», «хвилювання громадськості» і «поширення неправдивих чуток». Так, в 2004 році блогер був арештований за

повідомлення про арешт трьох інших користувачів. В 2012 році за обвинуваченням у поширенні дезінформації був арештований адміністратор сайту, що повідомляв про курс національної валюти стосовно долара.

За заявою представника офіційної влади, в 2006 році в Ірані були блоковані більше 10 мільйонів сайтів, 90% з яких належали до «аморального контенту». Порнографія залишається одним з головних пріоритетів для блокування. При цьому до неї Іран відносить навіть зображення провокаційного одягу. Пошукові запити, що містять слова «секс», «жінка» і «фотографія» фарсі або англійською, також блокуються. Фільтруються й багато інших сайтів, близьких до цієї тематики, зокрема сайти знайомств, матеріали про статеву освіту й ресурси ЛГБТ-співтовариств.

Станом на 2016 рік в Ірані блоковано найбільші міжнародні інтернет-сервіси, такі як Facebook, YouTube, Twitter і Flicker. Доступ до сервісів Google періодично зникає, що ускладнює їх використання. Заблоковано більшість платформ для ведення блогів, у тому числі Livejournal і Xanga.

В 2011 році іранська влада оголосила про плани зі створення Національного Інтернету, що передбачають захист країни від кіберзагроз, обмеження доступу користувачів до контенту за кордоном, а також більш суворий контроль за їхніми діями. Ініціатива припускає створення національних аналогів пошукових систем, поштових сервісів і платформ для ведення блогів. Брак офіційної інформації призвів до появи різних версій того, які цілі переслідує Іран. За однією з них, під Національним Інтернетом мається на увазі мережа, повністю ізольована від глобальної, на зразок діючої в Північній Кореї. У той же час представники влади заявили, що як базову модель обрано регулювання Інтернету в Китаї, коли весь зовнішній трафік суворо контролюється, але доступ до нього зберігається.

*Інтернет-цензура в Китаї*

Коли мова заходить про систематичне цензурування інтернет-контенту на державному рівні, майже завжди наводиться приклад Китаю – країни, де заборонено нібито практично все. Однак, як це часто буває, реальність виявляється набагато складнішою, ніж створений міф.

Насамперед, для аналізу китайської моделі блокування контенту в Мережі необхідно зупинитися на тому, що взагалі являє собою китайський сегмент Інтернету. Сьогодні Китай з 564 мільйонами інтернет-користувачів посідає перше місце у світі за даним показником, а рівень їхньої активності в Мережі не тільки не поступається, але й у деяких сегментах значно перевершує активність громадян інших держав, незважаючи на відсутність доступу до популярних міжнародних комунікаційних сервісів. Аналогічною є ситуація й у комерційній складовій Мережі – Китай не поступається країнам Європи в частині розвитку розважального й комерційного сегментів: існують великі торговельні площадки, розвинено систему мікроплатежів, а ринок онлайн-ігор посідає перше місце за обсягом у світі, з величезною кількістю локальних продуктів.

У той же час гігантський з погляду аудиторних і фінансових параметрів

інтернет-сектор Китаю уживається зі складною системою цензури, що складається з трьох базових елементів: 1) система фільтрації трафіка «Золотий щит» (вона ж «Великий китайський фаєрвол»); 2) система блокування пошуку небажаної інформації; 3) ручна система фільтрації контенту, що публікується в соціальних мережах і блогосфері.

*«Золотий щит», він же «Великий китайський фаєрвол»* – це система фільтрації інтернет-контенту, розробка якої почалася в 1998 році, а офіційний запуск відбувся в 2003. За оцінками експертів, вартість її створення могла скласти до $ 800 млн., а в її розробці брали участь великі американські корпорації, зокрема IBM. Завданням «Золотого щита» є блокування доступу користувачів з материкового Китаю до деяких інтернет-ресурсів, розташованих на серверах за межами країни. Список заборонених ресурсів формується безпосередньо в Пекіні, й у нього входять як сайти політичної спрямованості, так і світові соціальні сервіси, непідконтрольні пекінській владі.

На початок минулого року було відомо про приблизно 2600 сайтів, доступ до яких заблоковано за допомогою системи «Золотий щит». Сорок п’ять з цих сайтів входять у список 1000 найбільш відвідуваних у світі інтернет-сайтів за версією сервісу статистики Alexa. Так, у списку заблокованих перебувають Facebook.com, Youtube.com, Twitter.com, Blogspot.com, Blogger.com, Vimeo.com, Nytimes.com, WordPress.com, а також найбільші порнографічні ресурси Мережі. Найбільші російські соціальні мережі «В контакте» і «Одноклассники» доступні китайським користувачам, однак лише тому, що місцеві жителі ними практично не користуються.

Доступ до деяких сайтів обмежений лише частково. Так, китайським користувачам доступний сайт Вікіпедії, однак відсутній доступ до статей, що зачіпають питання китайської політики. Аналогічна ситуація спостерігалася з пошукачем Google, функції якого були доступні лише частково, перш ніж компанія вирішила взагалі припинити свою роботу в материковому Китаї.

Технологічно «Золотий щит» передбачає такі методи фільтрації:

1) блокування IP-адреси;

2) фільтрація DNS-запитів та їх переадресація;

3) блокування інтернет-адрес (URL);

4) фільтрація на етапі пересилання пакетів;

5) блокування з’єднань, здійснюваних через VPN.

Таким чином, «Золотий щит» сполучає у собі практично всі можливі на сьогодні технічні методи фільтрації, використовуючи їх вибірково стосовно тих або інших ресурсів. Це підвищує гнучкість і точність інтернет-цензури: одні ресурси можуть блокуватися повністю, а інші лише частково. Пакети і блокування VPN і TOR-з'єднань, у свою чергу, ускладнюють обхід державних фільтрів для рядових користувачів.

Втім, незважаючи на поширену думку, китайські інтернет-користувачі зовсім не страждають від нестачі сервісів комунікації. З моменту запуску системи «Золотий щит» найбільші локальні компанії безупинно копіюють найбільш успішні західні інтернет-продукти. Так, у Китаї існують практично повні (а найчастіше навіть удосконалені) аналоги сервісів Google (Baidu),

Facebook (RenRen), Twitter (Sina Weibo), YouTube (Tudou, YouKu), Wikipedia (Baike). Аналогами комерційних сервісів Amazon і eBay є, відповідно, портали Dangdang і Taobao.

Масштаби використання даних сервісів є колосальними: так, сервісом мікроблогів Sina Weibo регулярно користуються приблизно 300 млн. осіб, що перевищує аналогічний показник усього світового Twitter. Більшість суспільно-політичних дискусій, що відбуваються в китайському сегменті Інтернету, зосереджені переважно в цьому сервісі, причиною чого частково є особливості китайської мови (один китайський твіт зі 140 символів дорівнює за кількістю інформації приблизно чотирьом англійським), а також реалізована система коментарів до твітів, що більше нагадує Facebook. Таким чином, з погляду змістовної насиченості, китайські мікроблоги скоріше є ближчими до «великої» блогосфери, ніж до «твіттеру» в американському його розумінні.

Незважаючи на те, що основний вантаж цензури припадає на другий і третій рівень системи, вони були б неможливі без існування «Золотого щита». Ключове завдання цього державного «фаєрволла» – це не блокування доступу китайських користувачів до політичної інформації, розміщеної на закордонних сайтах, а створення умов для державного контролю над ключовими учасниками китайського інтернет-ринку. Саме тому блокуванню піддаються, насамперед, глобальні соціальні сервіси, призначені для обміну інформацією між людьми, а аж ніяк не політичні ресурси.

Завданням китайського уряду є максимізація можливостей з керування тим, що і як публікується в національному сегменті Інтернету, без тотального обмеження громадян на самовираження у Мережі. «Золотий щит» вирішує це завдання, створюючи ситуацію, за якої найбільші пошукові системи й соціальні сервіси належать китайським компаніям (переважно приватним) і розташовані на китайських серверах. Тим самим, головний «важіль» завжди перебуває в руках держави.

*Блокування пошуку небажаної інформації.* На всі пошукові системи, що працюють у китайському сегменті Інтернету, поширюються правила фільтрації пошукової видачі за рядом ключових запитів.

Можливо поділити всі заблоковані ключові фрази на дві групи: постійні й тимчасові. Постійне блокування стосується найбільш чутливих тим, пов'язаних із критикою Комуністичної партії Китаю й питанням прав людини. Приклади постійно заблокованих ключових слів: «демократія», «права людини», «диктатура», «мітинг», «червоний терор», «репресії», «незалежність Тибету» тощо. Також у списку заблокованих пошукових запитів – більшість імен китайських дисидентів і лідерів забороненого релігійного культу Фалуньгун. Примітно, що серед заблокованих пошукових запитів є й словосполучення «китайсько-російська границя», що пов'язане з поширеною критикою на адресу уряду з боку користувачів, що вважають демаркацію границі між двома країнами зрадництвом національних інтересів.

Тимчасовому блокуванню піддаються слова й фрази, пов'язані з обмеженими в часі кризовими ситуаціями, незалежно від їх характеру. Може йтися про політичні виступи, екологічні лиха або корупційні скандали.

Пошукові обмеження поширюються не тільки на спеціалізовані пошукові системи. Аналогічні правила діють й у найбільших китайських соціальних сервісах, зокрема у сервісі мікроблогів Sina Weibo.

*Фільтрація контенту в соціальних медіа.* Незважаючи на те, що в публічному полі переважно обговорюється «Великий китайський фаєрволл», ключову роль у фільтрації контенту грає зовсім не він, а десятки тисяч інтернет-цензорів, які вручну переглядають і фільтрують повідомлення, що публікуються сотнями мільйонів китайських інтернет-користувачів у блогах і соціальних мережах.

За останні роки було опубліковано два ключових дослідження, що дозволяють зрозуміти, як працює ця система: «How Censorship in China Allows Government Criticism but Silences Collective Expression», опублікований в American Political Science Review гарвардськими професорами Гаррі Кінгом, Дженніфером Пеном, Маргарет Робертс, і «Tracking and Quantifying Censorship on a Chinese Microblogging Site», підготовлений групою американських дослідників під керівництвом китайського незалежного експерта Тао Жу. В обох випадках аналіз проводився переважно на основі сервісу мікроблогів Sina Weibo як найбільш значимого інтернет-сервісу для суспільно-політичних дискусій у Сінетє (самоназва китайського сегмента Мережі).

В обох випадках дослідники дійшли висновку, що принципи функціонування й завдання китайської інтернет-цензури не є такими простими, як це прийнято вважати. Аналіз фільтрованих повідомлень показав, що метою китайської інтернет-цензури не є тотальне викорінювання якої-небудь політичної або громадської критики в соціальних мережах. Китайські користувачі не менше інших, у тому числі й російських, залишають критичні повідомлення на адресу уряду й чиновників, і ці повідомлення не цензоруються.

Цензори починають діяти, коли негативний для китайської влади інформаційний привід здобуває «вірусні» риси, загрожуючи перерости в масові політичні виступи, паніку або політичний рух, у тому числі віртуальний. Завданням є «зрізати» інформаційну хвилю, знизивши масштаб і гарячковість обговорення. І, у цілому, китайським «інтернет-поліцейським» це найчастіше вдається.

*Ця система складається з кількох рівнів:*

1) урядові інтернет-цензори;

2) регіональні інтернет-цензори;

3). цензори усередині великих інтернет-компаній.

Китайський уряд не розкриває дані про чисельність підрозділів «інтернет-поліції», але за різними даними на рівні уряду й регіональних центрів чисельність цензорів становить від 20 000 до 50 000 чоловік. У той же час основну роботу виконують не вони, а цензори, що працюють усередині інтернет-компаній. У найбільших компаніях, таких як Sina і Tencent, чисельність співробітників, у чиї обов'язки входить фільтрація контенту, досягає тисячі чоловік.

За допомогою масштабного аналізу й залучення складного технічного

інструментарію американськими дослідниками було виявлено як перелік тем, що підлягають цензуруванню, так і різні параметри, пов'язані з фільтрацією контенту.

Логіка втручання є такою: як тільки кількість повідомлень за якоюсь темою починає різко зростати, а сама тема здобуває характер «інформаційної хвилі», цензори вживають заходів для руйнування комунікативних зв'язків між користувачами й перешкоджають подальшому обговоренню теми. Через нетривалий час користувачі, що позбулися можливості публікувати й/або одержувати відгук аудиторії на свої повідомлення з боку інших користувачів, починають втрачати інтерес до теми.

Водночас у спокійній інформаційній ситуації, що не передвіщає масових політичних виступів та інформаційних скандалів, критика уряду, регіональних чиновників і різних явищ суспільно-політичного життя не забороняється. Більше того, на думку низки дослідників, китайський уряд з більшою увагою ставиться до критичних публікацій блогерів, особливо в частині критики регіональних чиновників, сприймаючи це як один із ключових елементів необхідного «зворотного зв'язку» для керування країною.

Інструменти фільтрації контенту в рамках Sina Weibo можна розділити на три категорії: проактивні, реактивні та інші.

До проактивних інструментів фільтрації належать:

- запобігання відправленню повідомлень. У цьому випадку при відправленні повідомлення Weibo інформує користувача, що в повідомленні міститься контент, який порушує правила сервісу й не може бути опублікований;

- премодерація повідомлень. У цьому випадку Weibo приймає до відправлення повідомлення, однак інформує користувача, що воно буде опубліковане протягом декількох хвилин. Цей час потрібно для ручної перевірки контенту цензорами;

- приховування повідомлень від інших користувачів при публікації. Weibo публікує повідомлення, однак робить його невидимим для інших користувачів. У цьому випадку автор повідомлення ніяк не інформується про подібний статус його публікації.

Реактивні інструменти:

- видалення раніше опублікованих повідомлень. Разом з оригінальним повідомленням видаляються протягом декількох хвилин і всі «репости» й коментарі до нього;

- закриття аккаунтів найбільш «шкідливих» користувачів.

Інше:

- обмеження пошуку по сервісу мікроблогів.

При «реактивному» видаленні повідомлень за темою велика їхня кількість видаляється протягом години після публікації. Приблизно 90% повідомлень, що цензоруються, включаючи репости й коментарі, видаляються протягом доби після їх публікації.

Втім китайські користувачі соціальних сервісів швидко навчилися обходити обмеження блокування тих або інших слів і виразів за допомогою

особливостей китайської мови. Так, ієрогліф «цензура» у Мережі заміняють ієрогліфом «річковий краб», що при різному написанні однаково вимовляється. Аналогічна ситуація й з іншими формально забороненими словами. Однак подібні виверти можуть утруднити роботу цензорів, але не роблять її неможливою. При виникненні кризової інформаційної ситуації замаскований контент також піддається видаленню.

При виникненні потенційно небезпечної «інформаційної хвилі» уживають заходів, спрямованих не тільки на фільтрацію окремих повідомлень, але й на ліквідацію ключових джерел негативної інформації. Акаунти найбільш активних блогерів видаляються, а самі вони можуть піддатися переслідуванню з боку правоохоронних органів. Втім строки арешту для блогерів, як правило, невеликі - від кількох днів до місяця.

Зрозуміло, цензори не в змозі вручну відслідковувати абсолютно всі повідомлення, що публікуються в системі мікроблогів. Моніторинг здійснюється двома шляхами: по-перше, за допомогою пошуку ключових слів, що належать до фільтрованої теми, включаючи слова-замінники, використовувані користувачами для обходу системи фільтрації контенту; другий спосіб - це персональний моніторинг найбільш «неблагонадійних» користувачів, раніше помічених в обговоренні чутливих для китайської влади тем, і їхній поведінці приділяється найбільш пильна увага.

Американським дослідникам удалося виділити теми, повідомлення з яких піддавалися цензурі в період з липня по серпень 2012 року:

- антиросійські й антикитайські заяви сірійських бойовиків;
- екологічні протести в східному Китаї з приводу будівництва трубопроводу;
- повторний арешт Чі правозахисника Гуїжі;
- фотографії групового сексу за участю регіональних чиновників;
- побиття японського кореспондента, що брав інтерв'ю в учасників політичних протестів;
- чутки про обвалення однієї зі станцій метро в Пекіні;
- обговорення висловлень колишнього прем'єр-міністра Китаю Вена Дзябао про політичні реформи в Китаї в ефірі телеканалу CNN;
- протести в Гонконгу проти запровадженого в школах курсу «національної освіти»;
- смерть матері й дитини в результаті примусового аборту, зробленого в рамках політики «одна родина - одна дитина».

Як уже було зазначено, повідомлення з вищевказаних тем цензоруються однаково в той момент, коли вони набули характеру «інформаційної хвилі» і могли призвести до масових виступів. Після того як розпалювання теми спадає, активність цензорів поступово припиняється.

Варто зазначити, що подібна система цензури існує не тільки в Sina Weibo та інших великих загальнонаціональних інтернет-сервісах. Цензоруються й повідомлення, що залишаються на численних й популярних в Китаї регіональних і муніципальних інтернет-форумах. У цьому випадку процес видалення небажаних записів займає трохи більше часу, але однаково

переважна більшість небажаного контенту видаляється протягом доби.

Втім, незважаючи на наявність настільки масштабної й багаторівневої системи контролю за контентом у Мережі, китайська влада регулярно виступає із ініціативами із запровадження нових елементів, покликаних відгородити громадян від небажаної інформації. Найцікавішою ініціативою подібного роду можна назвати програмний комплекс «Зелена дамба», запущений у 2009 році.

Передбачалося, що встановлення даної програми буде обов'язковим на всіх персональних комп'ютерах, які були у продажу в Китаї з 1 липня 2009 року. Однак спершу уряд КНР вирішив відкласти дату запуску системи через численні технічні проблеми і той факт, що виробники комп'ютерів не встигали встановити програму на свою продукцію. Втім, уже в серпні 2009 року було ухвалено рішення зробити встановлення «Зеленої дамби» необов'язковим, а до кінця 2010 року уряд відмовився від даного проекту зовсім, пообіцявши, однак, що в майбутньому повернеться до цього питання.

Наприкінці 2012 року була розпочата ще одна спроба посилення державного контролю над інтернет-простором. Влада Китаю вирішила скористатися досвідом сусідньої Південної Кореї й провести масштабну деанонімізацію китайської блогосфери. Було прийнято закон, що зобов'язує користувачів реєструватися в соціальних сервісах, таких як Sina Weibo, під своїми справжніми іменами. Ті користувачі, які зареєструвалися раніше, також повинні були повідомити свої паспортні дані операторам сервісів. Проте через деякий час з'ясувалося, що недотримання даної норми не призводить до яких-небудь санкцій, тому значна частина блогерів зволіла зберегти свій анонімний статус.

## 2. Моделі фільтрації контенту в Інтернеті

Закони, що регулюють Інтернет, застосовувані методи фільтрації і контент, що блокується, є специфічними для кожної держави. Проте існують групи країн, які переслідують схожі цілі в питаннях інтернет-цензури. На підставі спільності завдань і доводів, що використовують ці країни для обґрунтування втручання в Інтернет, а також схожості інструментів, які вирішують дане завдання, можливо виділити 5 моделей цензури. При цьому окремі держави можуть демонструвати характерні ознаки відразу двох моделей.

***Азіатська модель***

*Характерна риса*: розпливчасте визначення категорій контенту, що блокується, який надає уряду широкі можливості в галузі цензури.

*Приклади країн*: Китай, В'єтнам, Південна Корея, Сінгапур.

*Мета і завдання фільтрації Інтернету*: незважаючи на істотні розходження в політичному устрої зазначених держав, загальною рисою цих країн є переважна точка зору на головну роль держави, що повинна обмежувати доступ своїх громадян до небажаної інформації. Закони, що регулюють Інтернет, прямо вказують на головну роль держави в охороні суспільних відносин і національної безпеки. У Китаї визначено 9 категорій інформації, що розглядається як шкідлива, у тому числі для «національної єдності». В'єтнам забороняє «зловживання демократичними свободами на шкоду інтересам держави»; Південна Корея - інформацію, що порушує «громадський спокій і порядок, мораль і гарні традиції». У Сінгапурі завданням агентства, що регулює пресу, є запобігання появі матеріалів «проти суспільних інтересів, порядку й національної гармонії».

*Категорії контенту, що блокується*. Розпливчасте визначення матеріалу, який вважається забороненим, надає урядам країн широкі повноваження в трактуванні законів. Пріоритет віддається політичному контенту й інформації, що блокується з міркувань безпеки. Китай фільтрує найбільш широкий спектр чутливих тем - починаючи від незалежності Тайваню й закінчуючи духовним рухом Фалуньгун. Особливо ретельно блокуються міжнародні сайти, що містять критику Комуністичної партії Китаю, і популярні соціальні сервіси. Схожа картина спостерігається й у В'єтнамі, де головним об'єктом цензури виступають сайти, що піддають сумніву керівну роль його влади. Південна Корея блокує вузьку категорію контенту, але робить це з високою ефективністю - під забороною все, що пов'язано з північним сусідом, а також окремі антидержавні матеріали.

Крім боротьби із сайтами в Інтернеті, кримінальному переслідуванню піддаються користувачі, що залишають повідомлення з похвалою Північної Кореї в соціальних мережах. У Південній Кореї також активно борються з порушеннями авторських прав - з 2009 року там діє закон «про три попередження». Він передбачає відключення від Інтернету користувачів, які систематично завантажують нелегальну продукцію. Влада Сінгапуру вбачає одну з основних загроз у расизмі - населення острова багатонаціональне й там

проживає значна кількість іноземців. У 2005 році троє користувачів були заарештовані відповідно до «Акта про підбурювання» за расистські повідомлення в Інтернеті.

Незважаючи на те, що формально порнографія належить до контенту, який фільтрується у всіх країнах цієї групи, дослідження OpenNet показало, що там недоступною є незначна частина таких сайтів. Лише Китай здійснив у 2010 році широку кампанію з блокування порнографічних матеріалів та онлайн-казіно. У Сінгапурі символічно заблоковано лише кілька сайтів з порнографією.

*Використовувані методи фільтрації.*

Основні методи, на які покладаються уряди країн даної групи, - самоцензура й збір інформації в Інтернеті. Всі користувачі Південної Кореї, що використовують великі сайти, донедавна повинні були реєструватися під своїм справжнім ім'ям. Сінгапур зобов'язує проходити процедуру реєстрації не тільки інтернет-провайдерів, але й користувачів, «що поширюють або обговорюють політичну або релігійну інформацію, пов'язану із Сінгапуром». І в Китаї, і у В'єтнамі урядові агентства здійснюють активне стеження в Інтернеті й регулюють роботу інтернет-провайдерів.

З огляду на те, що в цих державах користувачі неодноразово піддавалися кримінальному переслідуванню за висловлювання в Інтернеті, такі заходи дозволяють жорстко контролювати хід онлайн-дискусій. Крім того, країни застосовують системи технічної фільтрації різної складності. Якщо Китай володіє найсучаснішою на сьогодні системою «Золотий щит», яка використовує всі методи фільтрації, то В'єтнам і Південна Корея покладаються на простіші способи. Так, В'єтнам застосовує перекручування DNS-записів, а влада Південної Кореї делегує видалення небажаного контенту провайдерам.

Характерна риса систем фільтрації даної групи країн - застосування комерційного програмного забезпечення західних IT-компаній. Саудівська Аравія й Оман використовують SmartFilter від McAfee, Катар - Netsweeper однойменної компанії. Інтернет-провайдери Індонезії блокують порнографію за допомогою HTTP проксі-серверів різних виробників. Перевагою такого підходу є те, що складання й відновлення блок-аркушів бере на себе постачальник програмного забезпечення. Як результат, Саудівській Аравії вдається блокувати значну частку порнографічних сайтів - вражаюче досягнення, якщо врахувати їхню кількість в Інтернеті. Його зворотним боком є те, що блокується переважно англомовний контент, тоді як ресурси арабською мовою зазнають обмежень в останню чергу. Крім технічних методів, країни активно переслідують порушників законів у Мережі. Комітет із захисту журналістів визнав Саудівську Аравію однією з найгірших країн для блогерів - за виступи із критикою держави користувачі регулярно піддаються кримінальному переслідуванню. Катар і Оман вдаються до арештів користувачів у менших масштабах. В Індонезії випадків кримінального переслідування блогерів мало - зокрема, один користувач був арештований за розміщення карикатури на пророка Мухаммеда на своїй сторінці в Facebook.

*Контент, що блокується з міркувань безпеки:*

- сайти, що порушують інтелектуальну власність. Особливо жорстке

законодавство в цій сфері діє у США. Великі пошукові системи, зокрема Google, фільтрують результати пошуку з урахуванням скарг правовласників;

- файлообмінні сайти, програми й торрент-трекери. У 2012 році під тиском американської влади був заблокований на той момент один із найбільш відвідуваних сайтів Інтернету - файлообмінний сервіс MegaUpload, а його створювачі були арештовані. Широко висвітлюється боротьба з торрент-трекерами (The Pirate Bay, Demonoid, IsoHunt), які формально не порушують закон, але сприяють нелегальному поширенню інтелектуальної власності;

- VoIP (Voice-over-IP) програми й сервіси, що дозволяють передавати голос по Інтернету, такі як Skype і «Mail.Ru Агент». В Об'єднаних Арабських Еміратах й Омані використання таких програм є нелегальним й карається великим штрафом або тюремним ув'язненням. Причина блокування VoIP програм двояка - з одного боку, дзвінки по них складніше відстежити й прослухати, з іншого, їх використання призводить до збитків компаній стаціонарного й стільникового зв'язку, які найчастіше пов'язані із правлячими колами;

- інтернет-інструменти й соціальні сервіси. Інструменти, що дозволяють обходити інтернет-цензуру. До цієї категорії потрапляють анонімайзери й сайти зі списками проксі-серверів, тому що вони можуть бути використані для обходу державних фільтрів;

- хакерські сайти й ресурси з інформацією про обхід інтернет-цензури;

- соціальні мережі, площадки для блогів і мікроблогів, хостинги відео й зображень. У Китаї заблоковано Twitter, Facebook, YouTube, WordPress і ряд інших подібних ресурсів, сервери яких розташовані за кордоном. У такий спосіб китайський уряд примушує своїх користувачів використовувати місцеві сервіси, які легше контролювати й фільтрувати інформацію у контенті;

- пошукові системи. Так, у Китаї й на Кубі блокуються американські пошукові системи Google і Bing;

- безкоштовні поштові сервіси.

- онлайн-перекладачі. Вони можуть бути використані як проксі-сервери для обходу цензури. Крім того, з їх допомогою користувачі можуть одержати доступ до небажаної інформації іноземними мовами, яку складно відстежити.

## 3. Методи фільтрації контенту в Інтернеті

### *Збір інформації в Інтернеті*

Хоча сам по собі збір інформації в Інтернеті не належить до фільтрації контенту, отримані таким методом дані можуть бути використані для виявлення користувачів, що одержують доступ до забороненого матеріалу, сайтів, що містять такі матеріали, і способів обходу інтернет-фільтрів.

*Зберігання логів і іншої технічної інформації*. У більшості країн прийнято закони, що зобов'язують інтернет-провайдерів зберігати інформацію про користувачів і відвіданих ними ресурсів. Поліція й спецслужби можуть використовувати цю інформацію для встановлення особи порушників в Інтернеті.

*Спостереження за інтернет-кафе*. З метою запобігання використанню інтернет-кафе для нелегальної діяльності в ряді країн до їхніх власників пред'являються жорсткі вимоги до забезпечення безпеки. Так, у Китаї й Італії користуватися інтернет-кафе можна тільки при пред'явленні паспорта, а власники зобов'язані зберігати записи про користувачів. У В'єтнамі й Бірмі в кожному інтернет-кафе повинна бути встановлена відеокамера.

*Системи інтернет-стеження*. Можливості з відстеження інтернет-трафіка передбачені законодавством практично всіх країн світу. У Росії діє СОРМ-2, що зобов'язує провайдерів установлювати спеціальний пристрій, який дозволяє спецслужбам відслідковувати трафік окремих користувачів. Аналогічна система за назвою CALEA діє й у США. Особливий інтерес становлять системи, здатні вивчати трафік цілої країни, використовуючи технологію глибокого аналізу пакетів (Deep Packet Inspection). За допомогою подібних систем можливо здійснювати спостереження за активністю користувачів, наприклад, визначаючи, які додатки й сервіси вони використовують і яку інформацію пересилають. Застосування таких систем суперечить праву громадян на приватне життя й заборонене в ЄС та Росії. Проте у цей час на міждержавному рівні тривають дебати про допустимість їх застосування з метою боротьби з тероризмом і порушенням авторських прав. Оскільки вивчення трафіка цілої країни вимагає значних обчислювальних потужностей, дозволити собі системи масового спостереження за Інтернетом можуть не всі держави. У США Агентство національної безпеки в рамках «Патріотичного акта» відслідковує активність у Мережі за допомогою суперкомп'ютерів NarusInsight. Китай використовує глибокий аналіз пакетів з метою інтернет-цензури; серед інших країн, помічених у такому застосуванні технології, - Іран і Туніс.

### *Технічні методи*

*Блокування за IP-адресою*. При застосуванні даного методу сервер, на якому перебуває небажаний матеріал, стає повністю недоступним для користувача. Головною перевагою цього методу є його простота - він може бути реалізований за допомогою базового мережевого обладнання, що використовується інтернет-провайдерами. Однак з урахуванням сучасних

технологій за однією IP-адресою можуть знаходитися тисячі сайтів, а також інших сервісів, таких як FTP або електронна пошта, тому його блокування призведе до того, що всі вони стануть недоступними. Через низьку точність даного методу країни застосовують його з обережністю. Блокування за IP-адресою легко обходиться за допомогою різних технічних рішень, зокрема, проксі-серверів і VPN.

*Перекручування DNS-записів*. При зверненні користувача до будь-якого сайту, комп'ютер надсилає запит до DNS-серверу для того, щоб перетворити доменне ім'я на IP-адресу. У разі застосування даного методу DNS-сервер повертає невірну адресу і сайт виявляється недоступним. Перекручування DNS-запису також може бути реалізоване без застосування додаткового устаткування. Її перевагою перед блокуванням за IP-адресою є більш висока точність - недоступним стає тільки один сайт на сервері. При цьому все одно відбувається надмірне блокування. Наприклад, Китай періодично позбавляє своїх користувачів доступу до CNN International через небажані новини, які там з'являються. Хоча ставиться мета фільтрації тільки однієї сторінки новини, інші сторінки сайту також стають недоступними. Перекручування DNS-записів легко обходиться користувачами - у налаштуваннях браузера досить указати альтернативний DNS-сервер або вручну прописати IP-адресу заблокованого сайту.

*Блокування за URL-адресою*. В HTTP-протоколі URL-адреса містить доменне ім'я сайту, а також параметри запиту. Вони можуть бути звірені зі списком заблокованих ключових слів, і у випадку відповідності зв'язок користувача із запитаним ресурсом розривається, або він перенаправляється на блок-сторінку. Даний метод є більш ефективним порівняно з блокуванням за IP-адресою й перекручуванням DNS-запису, але вимагає додаткового устаткування, тому що він використовує поверхневий аналіз пакетів. Його додатковою перевагою є те, що він здатний динамічно блокувати нові сторінки, якщо в їхній адресі містяться заборонені слова. Наприклад, у Китаї блокуються всі запити, що містять слова “falun” і “gong”. Однак при неправильному налаштування ключових слів точність методу різко погіршується - він може пропускати небажаний матеріал або, навпаки, допускати надмірне блокування. Блокування за URL-адресою неможна обійти за допомогою звичайних проксі-серверів - необхідні інструменти, які шифрують трафік, такі як VPN або TOR.

*Пакетна фільтрація*. Це найбільш складний і дорогий метод, тому що він вимагає застосування глибокого аналізу пакетів. На даний момент повноцінно реалізований він тільки в Китаї. При використанні пакетної фільтрації вивчаються не тільки заголовки пакетів, що містять URL-адресу, але й весь їхній зміст. У разі наявності заборонених слів зв'язок між користувачем і сервером розривається. Метод дозволяє фільтрувати небажаний контент не тільки у веб-сторінках, але й у всіх протоколах - електронній пошті, сервісах миттєвих повідомленнях та ін. Істотним недоліком даного методу є те, що застосування глибокого аналізу пакетів може призвести до зниження швидкості інтернет-з'єднання, що спостерігається при доступі з Китаю до закордонних інтернет-серверів. У цілому пакетна фільтрація має ті ж переваги й недоліки,

що й блокування за URL-адресою.

*Фільтрація через HTTP проксі-сервер*. Даний метод найчастіше використовується організаціями для підключення корпоративних мереж до Інтернету, але його можна використовувати для фільтрації Інтернету в рамках всієї країни. Гібридний варіант за назвою Cleanfeed ефективно застосовується у Великобританії й Канаді для боротьби з дитячою порнографією. Кожний запит користувача звіряється зі списком IP-адрес, що містять заборонені матеріали. Якщо збігів немає, то запит користувача відсилається прямо, інакше він перенаправляється на проксі-сервер громадської організації Internet Watch Foundation. Проксі-сервер одержує запитувану сторінку й аналізує її на наявність дитячої порнографії. Якщо сторінка не містить заборонених матеріалів, то користувач одержує до неї доступ, інакше - створюється видимість, що ресурс недоступний. Гібридні варіанти фільтрації через HTTP проксі-сервер дозволяють при низькій вартості точно блокувати вузькі категорії контенту. При цьому вони настільки ж легко обходяться, як і фільтрація за IP-адресою.

*Порушення роботи мережі*. В екстрених випадках, таких як масові заворушення, влада країни можуть піти на повне або часткове відключення Інтернету. Досягається це шляхом фізичного відключення роутерів з Мережі або ж зміни їхніх налаштувань, через що більша частина з'єднань скидається. Даний метод застосовувався в Єгипті у ході заворушень 2011 року, Лівії, Сирії й Бірмі. Проте досвід використання даного методу в ряді країн показує, що повне блокування доступу в Мережу найчастіше провокує додаткове зростання масових невдоволень.

*Фільтрація результатів пошуку*. У ряді країн, таких як Китай, Франція й Німеччина, працюючі там пошукові системи зобов'язані виключати з результатів пошуку посилання на заборонені матеріали. Так, у французьких і німецьких версіях Google з пошукових результатів виключаються посилання на неонацистські групи й інші матеріали, заборонені законом. Таким чином, користувачі не можуть знайти небажаний контент. Фільтрація результатів пошуку - один з основних методів боротьби з порушеннями авторських прав в Інтернеті. Даний метод обходять використанням інших пошукових систем - наприклад, міжнародна версія Google не виключає з результатів сайти неонацистських угруповань і при цьому доступна із Франції й Німеччини.

## 4. Варіанти розміщення систем технічної фільтрації

Обов'язковою умовою установки інтернет-фільтрів є їх розміщення на ключових ділянках мережі, через які проходить весь трафік. Тому можливі такі рівні установки інтернет-фільтрів:

*Міжнародний шлюз.* Цей варіант припускає централізований підхід до фільтрації контенту. Програмне й апаратне забезпечення встановлюється на ділянці, що з'єднує національну мережу з міжнародними магістралями. Перевагою даного методу є більш повний контроль і єдиноподібність підходу до цензури - політика фільтрації може оперативно коректуватися, а її зміни торкатимуться відразу всіх користувачів. Однак створення централізованої системи фільтрації Інтернету, здатної точно блокувати небажаний контент, вимагає істотних витрат, пропорційних обсягу зовнішнього трафіка. Даний метод використовуються більшістю мусульманських країн Близького сходу. У Китаї, Пакистані, Узбекистані й Ірані він застосовується разом з фільтрацією на рівні інтернет-провайдерів.

*Інтернет-провайдери*. Іншим підходом до цензури в Інтернеті є установка систем фільтрації всіма провайдерами країни. З питання, які ресурси підлягають блокуванню, вони орієнтуються на рішення судів, або на реєстр, що ведуть державні або недержавні органи. У разі якщо методи фільтрації не регламентуються, їхня реалізація залишається на розсуд кожної компанії. У результаті практика фільтрації може істотно варіюватися від провайдера до провайдера, як убік надлишкового, так і недостатнього блокування. Зокрема, у Росії через некоректну реалізацію вимог закону 139-ФЗ окремими компаніями для їхніх користувачів виявилися недоступні всі блоги на платформі WordPress. Фільтрація на рівні інтернет-провайдерів застосовується більшістю європейських країн, а також В'єтнамом, Бірмою й Південною Кореєю й низкою інших держав.

*Інтернет-сайти й мережі організацій*. Фільтрація на рівні мереж організацій найчастіше застосовується приватними компаніями для контролю використання Інтернету своїми співробітниками, але також використовується державами для регулювання роботи шкіл, бібліотек й урядових закладів. Так, у США відповідно до Акта про захист дітей в Інтернеті умовою одержання державних субсидій для шкіл і бібліотек є встановлення фільтрів, що обмежує доступ неповнолітніх до порнографії. Оскільки вимога не є обов'язковою для всіх установ, а закон передбачає відключення фільтрів на прохання дорослих користувачів, Акт не обмежує свободу слова, закріплену в Конституції США.

У державах, де за законом інтернет-сайти й сервіси відповідають за контент, розташований за їх користувачами, їхні власники наймають співробітників, відповідальних за цензуру, і встановлюють спеціальне програмне забезпечення, що відслідковує заборонений контент. Наприклад, в Китаї блог-платформа компанії Microsoft MSN Spaces не допускала назви блогів, що містять слова «демократія» і «свобода», автоматично відхиляючи такі варіанти. Сервіс мікроблогів Sina Weibo блокує записи з великого набору ключових слів, а в його штаті значаться сотні співробітників, що здійснюють

цензуру вручну.

*Індивідуальні комп'ютери*. Даний підхід передбачає встановлення програмного забезпечення для фільтрації безпосередньо на комп’ютери користувачів. Головною проблемою тут є труднощі відстеження того, щоб користувач не видалив або відключив фільтр. З урахуванням цього, найчастіше індивідуальні фільтри використовуються на комп'ютерах приватних компаній, які можуть технічно обмежити права своїх співробітників вносити зміни в налаштування, а також батьками для захисту дітей від небажаного контенту у Мережі. Спроби застосовувати даний підхід для державної цензури робив Китай. У планах його влади було встановлення програмного забезпечення «Зелена дамба» на всі комп'ютери країни, що блокує доступ до віддалено обновлюваного списку сайтів і здатного розпізнавати порнографічні зображення. Але через численні технічні труднощі державні органи відмовилися від цієї ініціативи.

## 5. Пошук власника медійного контенту.

*Пошук за IP-адресою.* IP-адреса – це неповторна, унікальна адреса комп'ютера або іншого пристрою, якого підключено до мережі Інтернет або локальної мережі. Іншими словами, під час поточного з'єднання, користувачеві мережі інтернет належить унікальна комбінація цифр, якої більше немає в жодного одного користувача у світі. Власне ця унікальна комбінація цифр і є IP адресою. IP-адреса може бути статичною або динамічною і призначається провайдером. Статична IP-адреса є постійною і не змінюється при кожному підключенні до мережі Інтернет. Динамічна IP-адреса може змінюватися при підключенні до мережі Інтернет (змінюється остання цифра в IP-адресі). Кілька комп'ютерів можуть мати одну IP-адресу, якщо підключені через один сервер, і матимуть IP-адреси ідентичні до серверної.

Управляє простором IP-адрес американська некомерційна організація IANA - «Адміністрація адресного простору Інтернет». Вона виділяє блоки IP-адрес регіональним реєстраторам. Вони, в свою чергу, ділять блоки адрес по великим провайдерам, які в свою чергу поділяють адреси серед дочірніх провайдерів і так далі, доти, доки одиночна IP-адреса не видається особі, коли вона відвідує Інтернет. Отже, чи можна знайти конкретну людину за IP-адресою? Теоретично в більшості випадків це можливо. На практиці ж пошук людини за IP-адресою - досить складне завдання через низку різних причин. Наприклад, якщо IP-адреса динамічна, необхідно визначити, кому з користувачів в час, який цікавить, було призначено дану IP-адреса, тобто потрібно отримати доступ до логів і бази користувачів інтернет-провайдера. До речі, на сервері провайдера ведеться запис всіх адрес, які відвідував користувач, яку інформацію і з яких сайтів отримує, куди що відправляє, що шукав тощо. Далі може виявитися, що IP-адреса видавалася мобільному пристрою, абонент якого не контрактник або він вимкнений, викинутий і т.д. І, зрештою, наявна IP-адреса може належати одному або кільком проксі-серверам. У даному випадку отримати доступ до їхніх логів буде практично не можливо, як власне і знайти людину за IP-адресою.

З викладено можна зробити висновок, що можливо визначити приналежність IP-адреси до країни і міста, тобто визначити провайдера інтернет-користувача, але не знайти людину за IP-адресою. Це можна зробити за допомогою Гео-IP-сервісів для визначення географічного розташування IP адреси або хоста. І це залежить від точності внесеної провайдерами інформації про свої мережі.

Таким чином, в ряді випадків 100% точність визначення місця розташування IP-адреси можлива тільки до рівня країни. Для подальшого пошуку людини за IP-адресою необхідно звернутися до його інтернет-провайдера. Інтернет-провайдери ж, як правило, не надають інформацію про власника IP-адреси, оскільки це порушує права людини і, відповідно, закон. На законних підставах така інформація надається лише працівникам правоохоронних органів і тільки у встановленому законом порядку.

*Пошук суб'єкта за допомогою сервіса Whois у відкритих джерелах.* WHOIS (від англ. Who is - «хто такий?") - мережевий протокол прикладного рівня, що базується на протоколі TCP (порт 43). WHOIS використовується для отримання інформації про доменне ім'я. Інформація, що видається, включає в себе ім'я сервера, ім'я власника та адресу з телефоном. Тут можна дізнатися дату реєстрації та її закінчення, а також реєстратора, де домен був зареєстрований. Наявність служби WHOIS повинно розчарувати тих, хто сподівався на повну анонімність в Інтернеті. Навпаки, тут залишаються і фіксуються всі сліди, що легко піддаються виявленню та аналізу. Основну частину їх і видає інтерфейс WHOIS. Крім всього іншого, сервіс WHOIS показує дані про IP-адресу.

Сервіс WHOIS володіє базою даних, що включає всіх реєстраторів доменів. До бази даних належать усі існуючі доменні імена. Програма працює за звичайним принципом: отримавши запит у вигляді доменного імені, вона просіює базу даних і видає результат. Дані про домени, інформація про IP-адреси, їх приналежність до мереж, інформація про реальні персони або організації - всі ці відомості можуть знадобитися для пошуку правопорушника у мережі Інтернет.

Загалом механізм пошуку порушника авторських прав у мережі Інтернет може виглядати таким чином:

1. За допомогою пошукових систем (Google, Meta, Yandex і т.д.) знайти піратський ресурс, який розповсюджує заборонений контент на території України.
2. За допомогою сервісу WHOIS на сайті 2ip.ua визначити всю можливу інформацію за даним ресурсом, тобто де знаходиться даний сайт (в якій країні), хто надає йому площадку для розміщення сайту (адреса, сайт, телефон хостера), коли зареєстроване доменне ім'я, хто реєстратор та його дані.
3. Підготувати офіційне звернення на ці організації можливо через отримання IP-адреси користувача або адміністратора сайту та за допомогою провайдера з'ясувати його адресу.

Можливо спробувати ще більш простіший метод. Переважна більшість сайтів з піратським контентом розміщують рекламу для монетизації сайту. Спроба зв'язатись з адміністратором сайту та пропозиція йому щодо розміщення своєї реклами надає потенційну можливість отримати реквізити банківської картки або розрахунковий рахунок для оплати реклами або інший спосіб оплати, за яким значно легше встановити власника.

## 6. Приблизний алгоритм відновлення знищеного контенту за допомогою програмних засобів

З метою приховування протиправної діяльності поширеною є ситуація, що пов’язана зі знищенням медійного контенту. Тому на етапі розслідування виникає необхідність у відновленні такої інформації.

У більшості випадків видалена інформація може бути відновлена за допомогою програмних засобів. Часто їх застосування не становить більшої складності, ніж використання типових програмних засобів обробки комп'ютерної інформації, призначених для вирішення повсякденних завдань: запису інформації на оптичний диск, архівації даних, роботи з файловими менеджерами і т. ін.

Основні аспекти відновлення комп'ютерних даних за допомогою програмних засобів наведено нижче.

Програми, призначені для відновлення даних, працюють в цілому за єдиним алгоритмом, що складається з таких основних дій.

1. Сканування жорстких дисків з метою визначення конфігурації логічних дисків.
2. Сканування певного розділу з метою пошуку видалених чи пошкоджених елементів даних.
3. Запис відібраних даних за новою адресою.

Програми часто включають в список таких, що підлягають відновленню, не тільки видалені користувачем файли, але й файли з «частковими» пошкодженнями, зокрема:

- з некоректним штампом дати і/або часу (Invalid Dates);
- з некоректним набором атрибутів (Invalid Attributes);
- з неправильно вказаним розміром (Invalid File Size);
- у найменуванні яких присутні неприпустимі символи (Invalid characters).

При виборі програми для відновлення комп’ютерної інформації необхідно враховувати:

- типи носіїв, які підтримує програма;
- файлові системи і формати запису (для носіїв типу CD/DVD), які підтримує програма;
- уміння опрацьовувати довгі імена файлів та кирилицю;
- можливість запуску із зовнішнього носія, без інсталяції на жорсткий диск;
- здатність працювати на рівні логічних дисків і розділів, а також на фізичному рівні;
- уміння відшукувати логічні диски, втрачені унаслідок руйнування таблиці розділів або проведення реконфігурування диска;
- здатність враховувати формат відновлюваних файлів.

Крім того, для деяких типів файлів існують спеціалізовані засоби відновлення. Наприклад, пошкоджений файл архіву у форматі RAR слід спочатку спробувати відновити засобами архіватора WINRAR, і лише потім

шукати інші способи його відновлення.

На момент проведення даного дослідження як найбільш перспективні нами виділено такі програмні продукти, які дозволяють успішно відновлювати видалену інформацію, – Drive Rescue і EasyRecovery Pro. На прикладі їх алгоритму роботи ми пропонуємо розглянути основні етапи відновлення даних.

### *Програма Drive Rescue*

Після запуску програми на екрані з'являється діалогове вікно з пропозицією обрати мову інтерфейсу. Потім необхідно обрати один з трьох основних варіантів роботи, натиснувши на відповідну кнопку (рис. 1.)

Recover deleted files (відновлення видалених файлів) — пошук і відновлення файлів, видалених стандартним засобами Windows (минувши «корзину» або в результаті очищення останньої);

Find lost data (Пошук втрачених даних) — пошук і відновлення файлів і каталогів, що стали недоступними в результаті яких-небудь некоректних дій користувача або помилок системи, а також в результаті «швидкого» форматування;

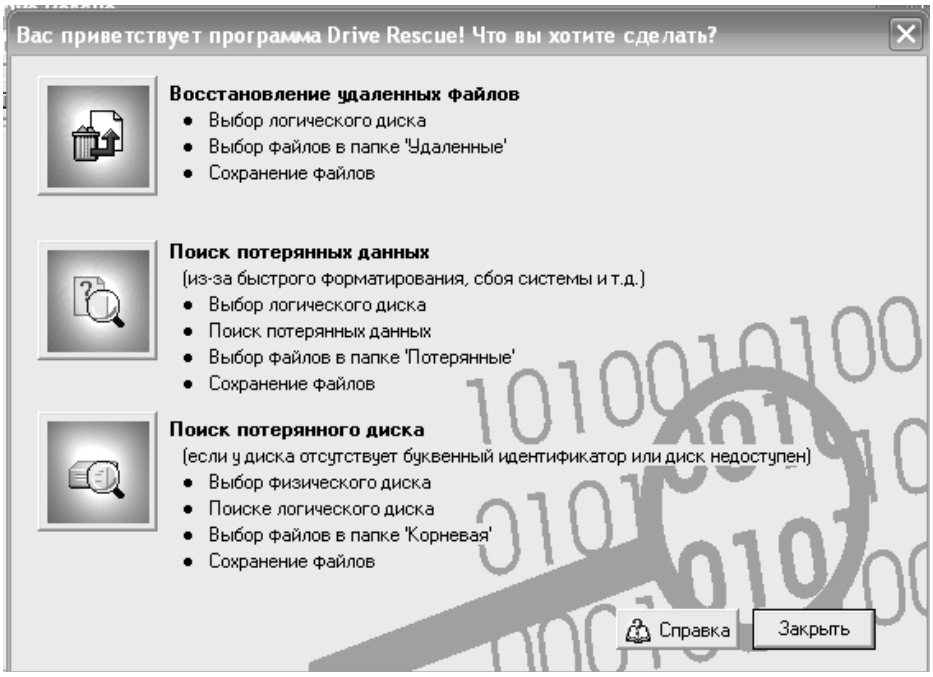
Find lost drive (пошук втрачених пристроїв) — пошук і відновлення логічних дисків, що стали недоступними в результаті яких-небудь некоректних дій користувача чи помилок системи (наприклад, в результаті псування таблиці розділів).

У будь-якому з трьох випадків Drive Rescue почне роботу зі сканування пристроїв (жорстких дисків, FDD, дисководів Jazz і Zip, а також накопичувачів типу Flash Card або SmartMedia) і виведе результати сканування в діалоговому вікні Select Drive (вибір пристрою) на вкладці Logical Drive (Логічний пристрій). Правда, результати сканування в кожному з трьох випадків можуть бути представлені різним чином (докладніше ці відмінності будуть розглянуті нижче).

Порядок подальших дій з відновлення даних залежить від конкретної ситуації. Найбільш типові випадки будуть розглянуто в подальших підрозділах. Можна відмовитися від запропонованого набору з трьох основних процедур, натиснувши кнопку Welcome to Drive Rescue на кнопці Close (Закрити) (див. рис. 1).

В цьому випадку ми отримаємо безпосередній доступ до основного вікна програми. Крім виклику довідки або отримання технічної підтримки через Інтернет можна скористатися однією з таких команд:

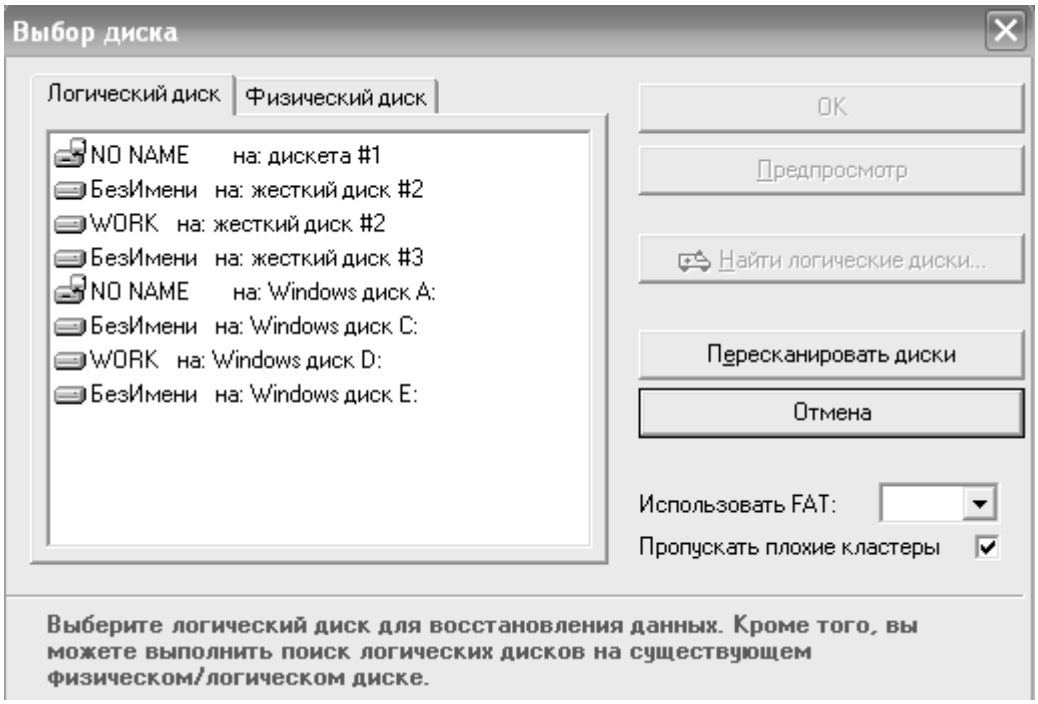
Рис. 1




Список логічних дисків, виявлених Drive Rescue

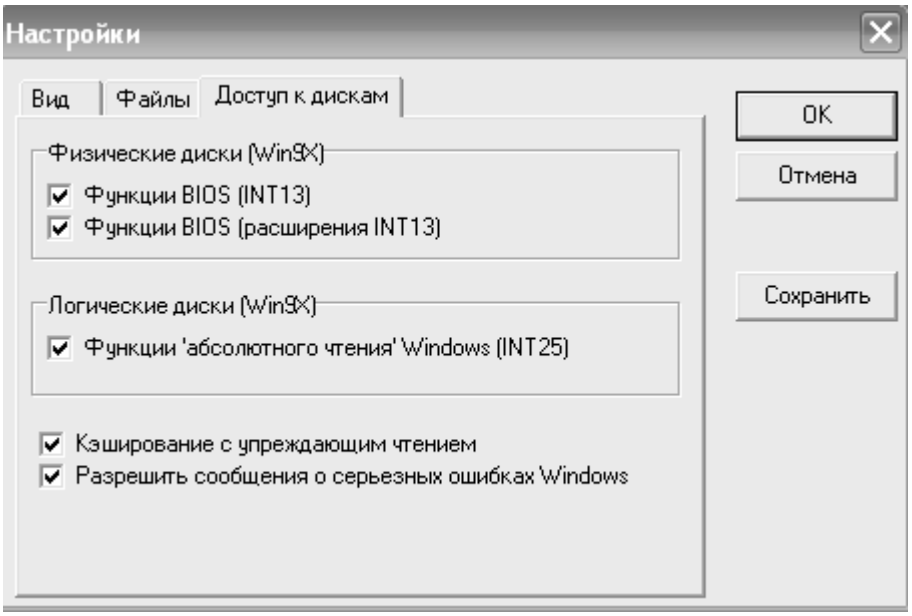
Object > Drive (Об'єкт > Пристрій) — ініціює процес сканування пристроїв, аналогічний тому, який може бути запущений з діалогового вікна Welcome to Drive Rescue;
Object > Options (Об'єкт > Параметри) — виклик вікна налаштування параметрів роботи Drive Rescue;
Info > System Info (Відомості > Відомості про систему) — виклик вікна, що містить відомості про апаратну і програмну конфігурацію системи.

Рис. 2.



З погляду роботи Drive Rescue з відновлення даних найбільший інтерес становить група параметрів, розміщених на вкладці Drive access (Доступні пристрої). Два прапорці з групи Physical drives (Фізичні диски) визначають, які засоби повинен використовувати Drive Rescue для прочитування даних з диска: стандартний сервіс BIOS (INT13), що використовує адресацію CHS, або розширений сервіс (INT13 Extension), який забезпечує повну підтримку LBA (рис. 3).

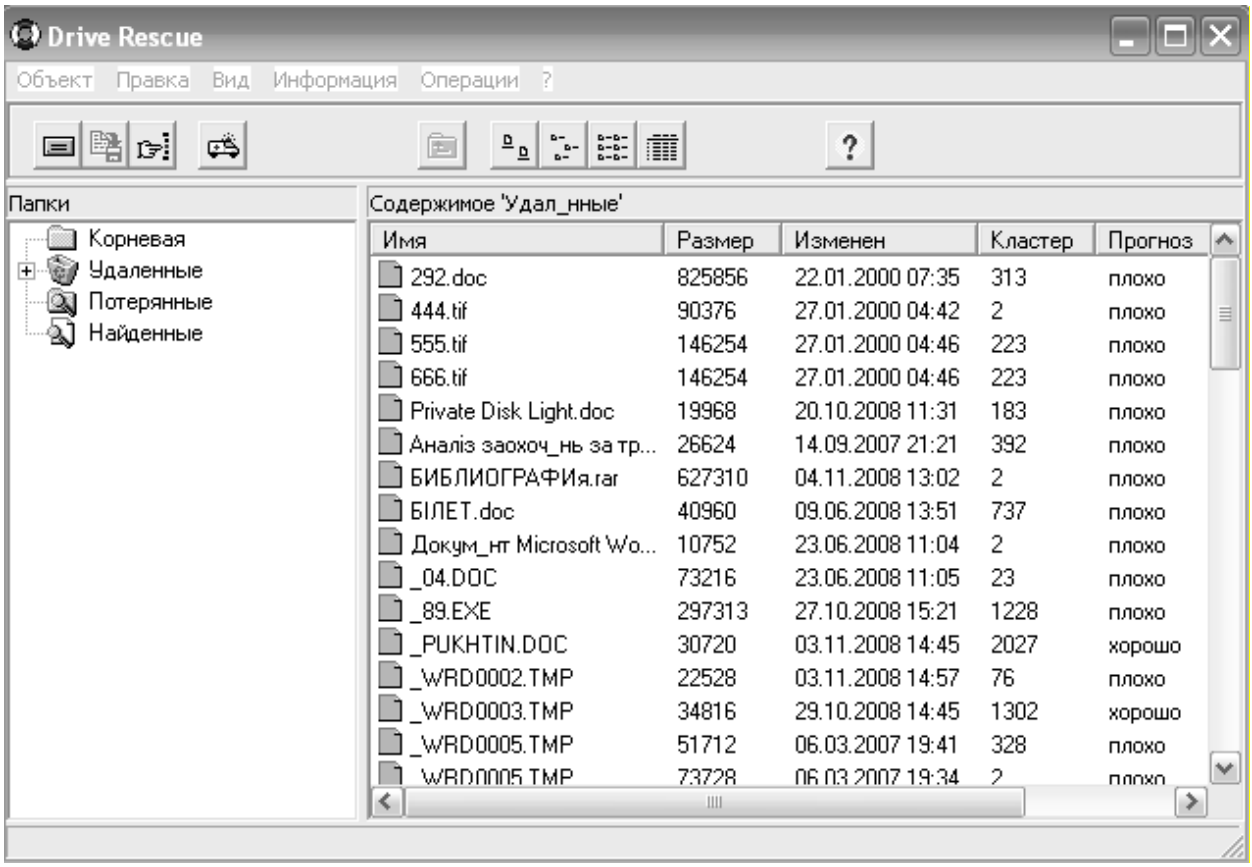
Рис. 3.




Відновлення видалених файлів і каталогів

Щоб ініціювати процедуру відновлення видалених файлів і/або каталогів слід натиснути у вікні Welcome to Drive Rescue кнопку Recover deleted files. Після завершення сканування пристроїв на екрані з’явиться список логічних дисків, виявлених Drive Rescue. Потім обрати диск, на якому був видалений файл (каталог), і натиснути розташовану праворуч від списку кнопку «ОК». В основному вікні програми будуть представлені результати аналізу диска (рис. 4).

Рис. 4.




У лівій частині вікна відображається дерево каталогів, що містить 4 основних гілки:

■ Root (Кореневий) — перелік вкладених каталогів і файлів, зареєстрованих в кореневому каталозі диска;

■ Deleted (Видалені) — перелік каталогів і файлів, помічених як видалені;

■ Lost (Втрачені) — список «втрачених» файлів і каталогів;

■ Searched (Знайдені) — список знайдених файлів; список формується в результаті виконання функції пошуку, про яку буде викладено нижче.

Щоб побачити вміст будь-якої гілки, слід натиснути на її значку мишею. Вміст відображається в правій частині вікна. При пошуку видалених файлів і каталогів Drive Rescue заповнює тільки гілки Root і Deleted.

Видалені об'єкти відмічаються в лівому і правому списках зеленим кольором. У правому списку, реалізованому у вигляді таблиці, можна отримати таку інформацію про видалений об'єкт:

■ Name (Ім'я) — ім'я об'єкта; у імені видаленого об'єкта можуть бути присутніми символи підкреслення, замінюючи втрачені символи початкового імені; в деяких випадках в списку можуть опинитися кілька однойменних файлів (наприклад, різні версії одного файлу); якщо потрібно відновити всі такі файли, заздалегідь їх потрібно перейменувати, обравши в контекстному меню команду Rename (Перейменувати);

■ Size (Розмір) — розмір файлу в байтах; потрібно мати на увазі, що

розмір зіпсованого файлу може не відповідати розміру файлу до видалення; іноді розмір файлу потрібно скоректувати вручну;

■ Date (Дата) — дата останньої зміни файлу;

■ Cluster (Кластер) — номер першого кластера файлу (каталогу); стовпець використовується при роботі з файловою системою FAT; для файлової системи NTFS замість нього використовується стовпець MFT Entry (Вхід MFT);

■ Condition (Стан) — стан видаленого файлу (каталогу) має такі можливі значення:

□ poor (поганий) — файл не може бути відновлений; проте така категорична оцінка не завжди справедлива: іноді файл, помічений як poor, все-таки вдається відновити;

□ fair (посередній) — файл може бути відновлений частково;

□ good (хороший) — файл може бути відновлений без втрат;

□ unknown (невідомо) — стан визначити не вдалося;

Type (Тип) — тип файлу відповідно до параметрів операційної системи.

Для відновлення видаленого об'єкта слід виконати такі дії.

1. Натиснути на його значку правою клавішею миші і в контекстному меню обрати команду Save to (Зберегти в).

2. У додатковому вікні (рис. 5):

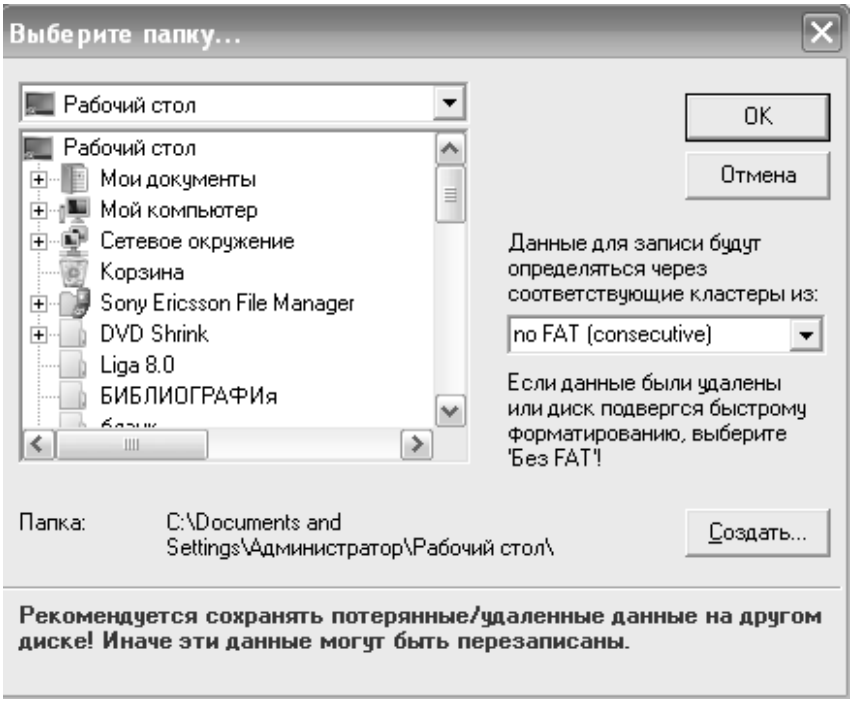
1) вказати диск і каталог, куди слід переписати відновлюваний об'єкт;

2) у списку, що розкривається, обрати пункт no FAT (consecutive) (Не використовувати FAT, переглядати послідовно);

3) натиснути кнопку ОК.

Потрібно пам'ятати, що відновлюваний об'єкт не можна записувати на той самий диск, на якому він розташований. Це може призвести до пошкодження розміщених на цьому диску як самого об'єкта, так і інших об'єктів, що підлягають відновленню.

Рис. 5



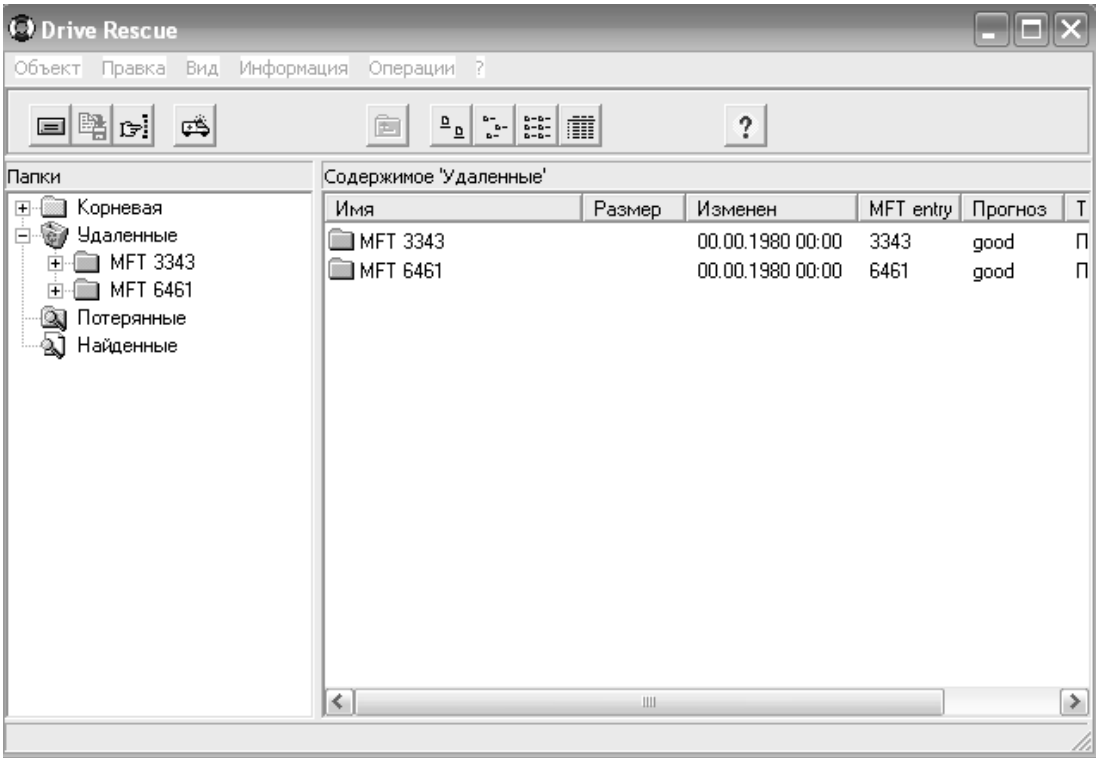

Після того, як видалений об'єкт був відновлений (записаний за новою

адресою), він автоматично видаляється з гілки Deleted.

Якщо пошук видалених файлів проводиться на диску з файловою системою NTFS, то результати пошуку виглядатимуть дещо інакше: знайдені об'єкти ідентифікуються за номерами записів (входів) до таблиці MFT (рис. 6). Відповідно в правому списку для знайдених об'єктів також указується не номер першого кластера, а номер запису в MFT.

В цілому технологія відновлення даних на NTFS-диску аналогічна технології, розглянутій для файлової системи FAT.

Рис. 6




Відновлення видалених файлів і каталогів

Виконання даної процедури може дещо розрізнятися залежно від причини втрати даних. У будь-якому разі процес пошуку потрібно починати зі сканування наявних пристроїв. У сформованому списку слід обрати диск, на якому розташовані видалені дані, і натиснути кнопку ОК.

Для продовження пошуку слід виконати такі дії.

1. У меню Tools (Сервіс) основного вікна програми обрати команду Find lost data (Пошук втрачених даних).

2. У вікні Select cluster range (Вибір діапазону кластерів) за допомогою регуляторів необхідно встановити діапазон кластерів, в якому слід здійснювати пошук (якщо необхідна інформація відсутня, краще здійснити його по всьому доступному дисковому просторові).

Стан процесу пошуку і поточні результати відображаються в додатковому вікні, в якому роздільно виводяться число втрачених каталогів і число втрачених файлів. Після завершення сканування всі знайдені об'єкти

поміщаються в гілку Lost основного вікна.

У лівому списку (Folders) представлено втрачені каталоги, що іменуються номерами їх перших кластерів.

У правому списку відображаються елементи, на які є посилання в обраному каталозі.

Якщо неможливо визначити за номером кластера відомості про те, який саме каталог нас цікавить, слід проглянути послідовно вміст всіх знайдених каталогів, обираючи їх по черзі в лівому списку; знайшовши потрібний каталог, слід запам'ятати або записати номер відповідного кластера.

Щоб відновити каталог, слід виконати такі дії.

1. Натиснути в лівому списку на значку гілки Lost; при цьому всі втрачені каталоги (впорядковані за номерами кластерів) будуть показані в правому списку.

2. Перейменувати каталог, давши йому осмислене ім'я; для цього натиснути правою клавішею миші в правому списку на значку каталогу (з номером записаного кластера), що цікавить, після чого в контекстному меню обрати команду Rename і відредагувати ім'я каталогу.

3. Натиснути в правому списку на значку каталогу правою клавішею миші і в контекстному меню обрати команду Save to.

4. У додатковому вікні (див. рис. 5) вказати диск і каталог, куди слід переписати відновлюваний каталог. У списку, що розкривається, оберіть номер копії таблиці FAT, в якому є найбільша впевненстьі (за умовчанням використовується перша, основна копія).

5. Натиснути кнопку «ОК».

Щоб відновити конкретний файл (або вкладений каталог) в каталозі, що цікавить, слід виконати таке.

1. У лівому списку натиснути на позначку каталога.

2. У правому списку перейменувати, якщо потрібно, відновлюваний файл.

3. Натиснути правою клавішею миші на значок файлу і в контекстному меню обрати команду Save to.

4. У додатковому вікні (див. рис. 5) вказати диск і каталог, куди слід переписати відновлюваний файл. У списку, що розкривається, обрати номер копії таблиці FAT, в якій є найбільша впевненість, і натиснути кнопку ОК.

Для деяких видалених файлів (наприклад, пошкоджених вірусом) в списку файлів може бути вказана нульова довжина. Існує вірогідність, що такий файл цілком «дієздатний», але недоступний для коректної роботи. Для його відновлення виконати такі дії.

5. Натиснути правою клавішею миші на значку файлу і в контекстному меню обрати команду Properties (властивості).

6. У додатковому вікні в полі Size (розмір) ввести відповідне значення (із запасом).

7. Зберегти файл описаним вище способом за новою адресою.

8. Відкрити файл за допомогою асоційованої з ним програми і зберегти його за допомогою команди Зберегти як (Save as).

Якщо Drive Rescue не може визначити розмір знайденого файлу, він

встановлює для нього розмір, вказаний в параметрах Drive Rescue, на вкладці Files (Файли) в полі Default file size (Розмір файлу за умовчанням).

### *Програма Easy Recovery Pro*

Інтерфейс Easy Recovery Pro реалізований так, щоб максимально полегшити користувачам доступ до основних функцій програми. Тому і знайомство з можливостями Easy Recovery зручно сумістити з описом інтерфейсу. Після завантаження програми на екрані з'являється вікно, в лівій частині якого розміщено меню у вигляді кнопок, що забезпечують доступ до чотирьох категорій функцій, а також до двох додаткових сервісів (рис. 7).

■ Disk Diagnostics (Діагностика диска) — утиліти для перевірки фізичних параметрів диска і цілісності файлової системи;

■ Data Recovery (Відновлення даних) — утиліти для пошуку і відновлення видалених і пошкоджених даних;

■ File Repair (Відновлення файлів) — спеціалізовані утиліти для відновлення файлів, створених додатками програми MS Office (окрім Outlook), а також ZIP-архівів;

Рис. 7

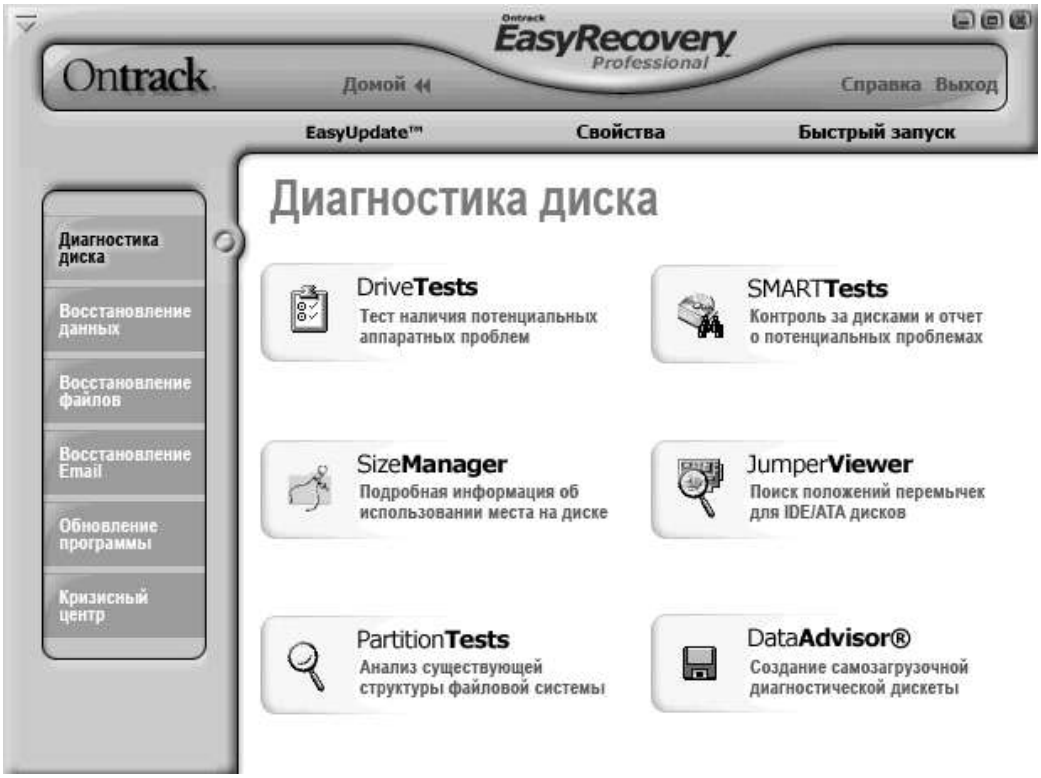

■ Email Repair (Відновлення файлів електронної пошти) спеціалізована утиліта для відновлення файлів Outlook;

■ Software Updates (Оновлення програми) — сервісні функції, що дозволяють отримувати інформацію і виконувати оновлення ліцензійної версії Easy Recovery через Інтернет;

■ Crisis Center (Кризовий центр) — набір функцій, що забезпечують доступ до сервісних веб-служб компанії Ontrack.

Щоб отримати доступ до конкретної функції з тієї або іншої категорії, досить натиснути на відповідній кнопці меню і потім обрати потрібну функцію в правій частині вікна; наприклад, на рис. 8 показано меню утиліт діагностування дисків.

Рис. 8




Коротка характеристика утиліт,
що входять до складу Easy Recovery Pro

■ Утиліта DriveTests дозволяє перевіряти фізичний стан дисків. Використовувані в ній варіанти тестування засновані на читанні записаних даних і дозволяють оцінити стабільність фізичних параметрів жорсткого диска. DriveTests включає два види тестів:

■ Quick Diagnostic Test (Швидкий діагностичний тест) — виконується протягом 90 секунд і забезпечує 90-процентну достовірність результатів тестування; його суть полягає в читанні секторів, обраних випадковим чином, але з урахуванням геометрії диска; за наслідками тестування видається одне з двох повідомлень: Pass (пройдений) або Fail (помилка); тест завершується при виявленні першого ж збійного сектора;

■ Full Diagnostic test (Повний діагностичний тест) — полягає в посекторному читанні всього диска;

■ повторна спроба; за наслідками тестування видається одне з трьох повідомлень: Pass (Пройдений), Passed with minor errors (Пройдений з мінімальним числом помилок) або Fail (Помилка); тест завершується достроково при виявленні 20 збійних секторів.

■ Утиліта SMARTTest дозволяє оцінити фізичні параметри диска на основі технології S.M.A.R.T.

Передбачено три варіанти тестування:

■ Return S.M.A.R.T. status (Повернення S.M.A.R.T.-состояния) — прочитування поточних показників диска відповідно до технології S.M.A.R.T.;

■ Run short Drive Self Test (Проведення скороченого самотестування диска) — припускає додаткове тестування диска в обмеженому режимі; тривалість тестування становить 1-2 хвилини;

■ Run extended Drive Self Test (Проведення розширеного самотестування диска) — припускає додаткове тестування диска в повному обсязі; тривалість тестування становить 20 хвилин або більше.

За наслідками всіх видів тестування формується докладний звіт. При виявленні тих або інших проблем звіт містить рекомендації з їх усунення. Всі тести можуть здійснюватися у фоновому режимі.

Утиліта PartitionTests призначена для проведення аналізу структури файлової системи диска. Вона виконує поглиблене обстеження елементів файлової системи з подальшою генерацією звіту про стан файлів даних. Для отримання коректних результатів рекомендується перед запуском утиліти закрити всі інші програми.

Загальним для всіх утиліт, що входять до складу Easy Recovery, є те, що вони працюють в режимі майстра: користувачеві пропонується вказати параметри виконання чергового кроку завдання і перейти до наступного кроку.
Категорія Data Recovery, до складу якої входять 6 утиліт:

■ DeletedRecovery — пошук і відновлення видалених файлів і каталогів;

■ AdvancedRecovery — пошук і відновлення видалених файлів і каталогів з можливістю додаткової настройки параметрів пошуку;

■ FormatRecovery — відновлення даних в розділах, які випадково відформатували або видалених розділах;

■ RawRecovery — відновлення даних в розділах з порушеною структурою;

■ ResumeRecovery — сервісна функція, що дозволяє зберігати поточні параметри відновлення з метою їх використання в повторних сеансах роботи з EasyRccovery;

■ EmergencyDiskette — утиліта для створення аварійного завантажувального гнучкого диска; такий диск містить системні файли дискової операційної системи Caldera DR-DOS, а також DOS-версію утиліт з категорії Data Recovery; утиліта має важливу перевагу і два істотних недоліки: з одного боку, вона дозволяє створювати завантажувальний диск безпосередньо з середовища Windows XP, з іншого — на створюваному диску відсутній драйвер з підтримкою кирилиці, і тому файли і каталоги з літерами кирилиці стають невпізнанними; крім того, після завантаження з гнучкого диска потрібно виконати ряд додаткових операцій в режимі командного рядка, що під силу не кожному «рядовому» користувачеві.

Перші чотири з названих утиліт безпосередньо пов'язані з відновленням даних і працюють в цілому за єдиним алгоритмом, що складається з таких основних дій.

1. Сканування жорстких дисків з метою визначення конфігурації логічних

дисків.

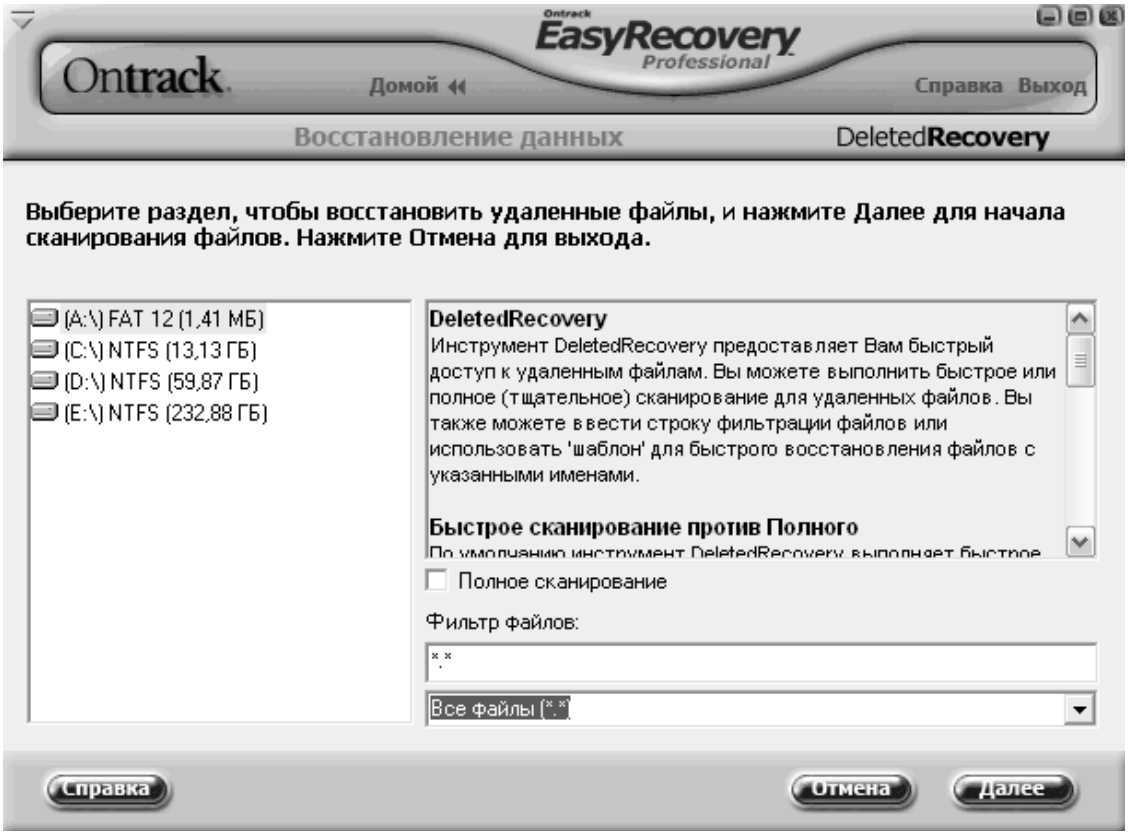
2. Сканування вказаного користувачем розділу з метою пошуку видалених або пошкоджених елементів даних.

3. Запис обраних користувачем даних за новою адресою.

Для відновлення даних за допомогою DeletedRecovery необхідно виконати такі дії.

1. У списку логічних дисків обрати той, на якому потрібно відновити видалені файли (рис. 9).

Рис.9




2. Щоб звузити діапазон пошуку в полі File Filter (Фільтр файлів) ввести з клавіатури або за допомогою розташованого нижче списку маску для пошуку файлів.

3. Якщо після видалення файлу спливло багато часу і він може бути пошкоджений, встановити прапорець Complete Scan (Повний перегляд) для здійснення повнішого аналізу диска.

4. Натиснути кнопку Next (Далі), щоб перейти до наступного кроку; Easy-Recovery просканує диск і видасть результати в наступному вікні.

5. У лівій частині вікна (у дереві каталогів) обрати каталог, де розташований відновлюваний файл, а в правому списку — натиснути на значок цього файлу.

6. Щоб полегшити перегляд списку слід скористатися фільтром відбору знайдених файлів. Для цього натиснути кнопку Filter Options (Параметри фільтру) і у вікні налаштувань встановити необхідні параметри.

7. Щоб знайти конкретний файл можна застосувати функцію пошуку, що викликається кнопкою Find (Пошук); як критерії пошуку можуть бути використані ім'я файлу, його розмір, дата створення, а також стан після видалення.

8. Якщо потрібно заздалегідь подивитися на вміст відновлюваного файлу, натиснути на кнопці View File (Попередній перегляд файлу).

9. Завершивши вибір відновлюваного файлу (або каталогу), перейти до наступного кроку. Він полягає в записі відновлюваного об'єкта за новою адресою; як додаткові параметри можна вказати (рис. 10) необхідність архівації файлу, генерації звіту і пересилки файлу на FTP-сервер.

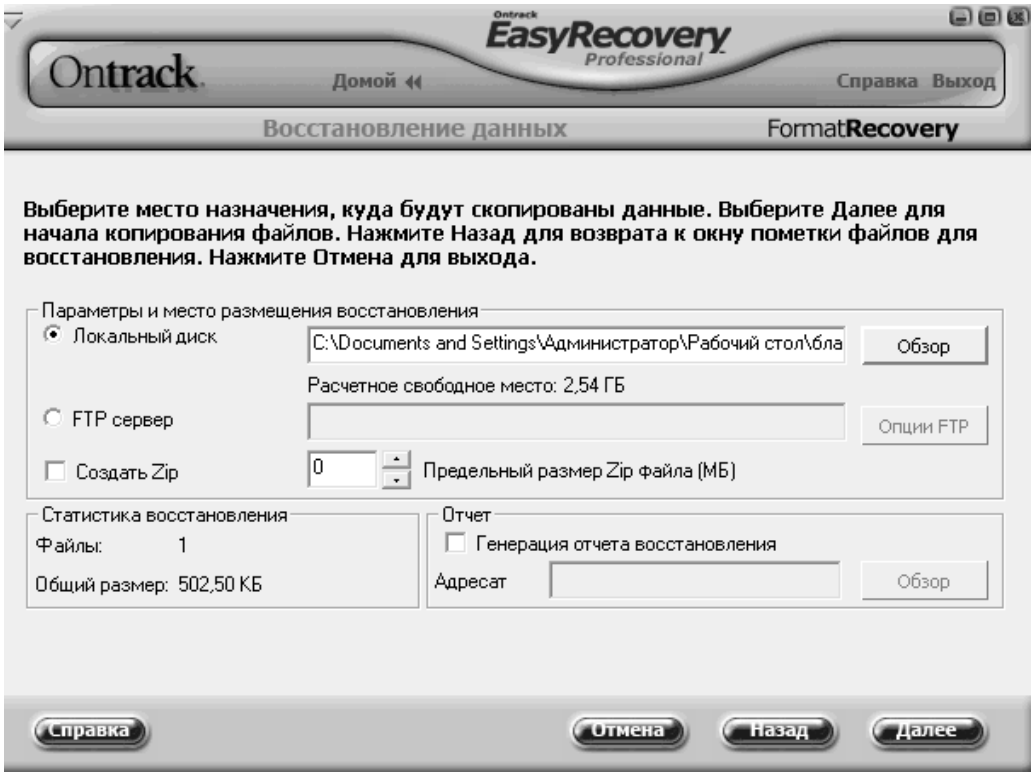
### *Відновлення даних за допомогою AdvancedRecovery*

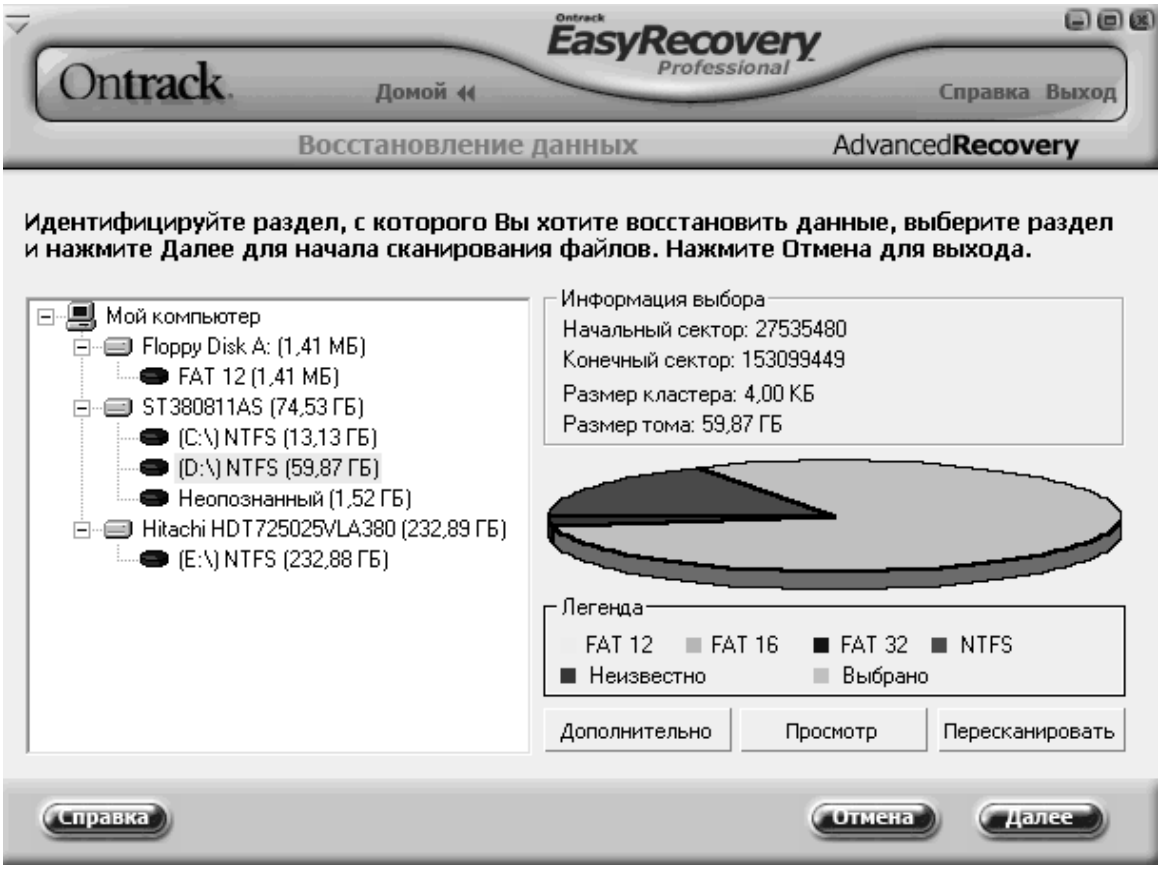
Основна відмінність AdvancedRecovery від утиліти DeletedRecovery полягає в можливості налаштування більшої кількості параметрів пошуку відновлюваних даних на логічному диску. Зокрема, користувач отримує можливість працювати не тільки з деревом каталогів, але й зі службовою інформацією розділу.

Після завершення сканування дисків AdvancedRecovery виводить на екран їх список і докладний звіт про параметри відповідного розділу (рис. 11).

Якщо програма AdvancedRecovery не змогла виявити який-небудь розділ або коректно визначити його параметри, можна змінити параметри сканування, задані за умовчанням.

Рис. 10






мал. 11

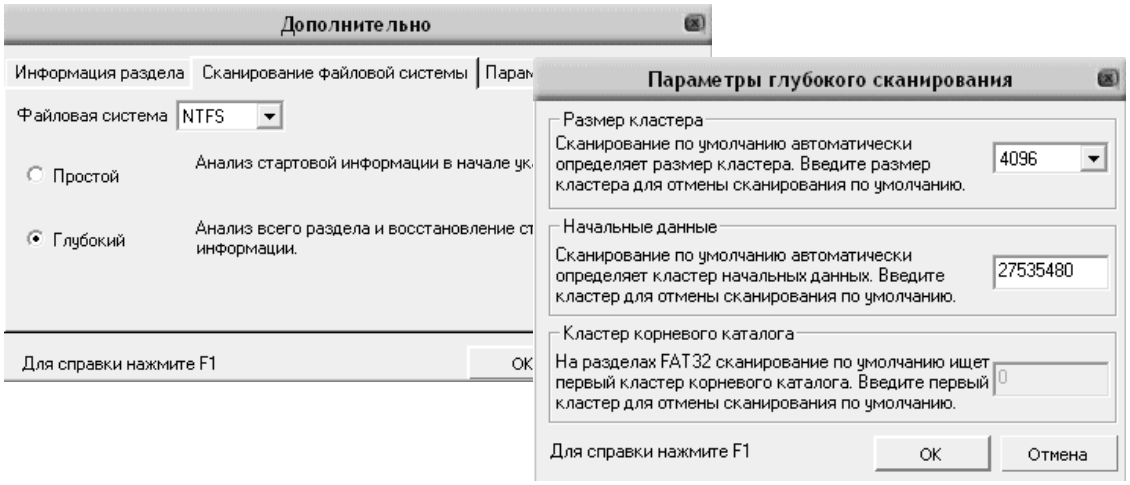
Для цього потрібно натиснути на кнопці Advanced Options (Додаткові параметри) і виконати необхідне налаштування в додатковому діалоговому вікні.

Вікно налаштувань містить чотири вкладки. Перша з них, Partition Information (Відомості про розділ) дозволяє змінити номери першого і останнього кластерів розділу, щоб «допомогти» AdvancedRecovery виявити його на диску. Крім того, натиснувши на кнопці Hint (Підказка), отримуємо можливість змінювати розміри (межі) одного або кількох розділів (рис. 12). Мається на увазі не реконфігурація дисків, а зміна меж, в рамках яких Advanced-Recovery повинен шукати втрачені розділи.

рис. 12

Вкладка File System Scan (Сканування файлової системи) дозволяє обрати тип і параметри файлової системи для обраного розділу, а також режим сканування (рис. 13).

Рис. 13




При виборі режиму Advanced Scan (Розширене сканування) можна додатково вказати розмір кластера, номер першого кластера області даних і (для файлової системи FAT) номер першого кластера кореневого каталогу.

Вкладка Partition Settings (Параметри розділу) містить єдиний елемент управління — список, що розкривається, за допомогою якого можливо обрати джерело відомостей про наявні в розділі дані. Це джерело використовуватиме в своїй роботі AdvancedRecovery.

Набір варіантів, наданих у списку, залежить від файлової системи досліджуваного розділу.

Для розділів FAT список містить такі варіанти:

■ Use FAT1 (Використовувати FAT1) — перегляд області даних виконується відповідно до інформації в першій копії FAT;

■ Use FAT2 (Використовувати FAT2) — пошук даних проводиться на основі другої копії FAT;

■ Use Best Math (Використовувати найбільш відповідну) — AdvancedRecovery спочатку порівнює фактичний вміст деякої частини диска з інформацією в обох копіях FAT, а потім застосовує для продовження роботи з диском найбільш відповідну копію FAT;

■ Ignore FAT (Ігнорувати FAT) — пошук даних проводиться па основі відомостей, що містяться в кореневому каталозі і в інших каталогах розділу; даний варіант доцільно застосовувати у тому випадку, коли обидві копії FAT зіпсовано (наприклад, в результаті швидкого форматування розділу).

Для розділів NTFS список містить два варіанти:

■ Use MFT (Використовувати MFT) — перегляд області даних виконується відповідно до записів в таблиці MFT;

■ Ignore MFT (Ігнорувати MFT) — аналіз диска проводиться без використання записів MFT.

■ Вкладка Recovery Options (параметри відновлення) дозволяє вказати Advanced Recovery, які файли слід включати в список тих, що підлягають

відновленню. За умовчанням до таких належать такі файли:

- з некоректним штампом дати і/або часу (Invalid Dates);
- з некоректним набором атрибутів (Invalid Attributes);
- з неправильно вказаним розміром (Invalid File Size);
- помічені як видалені (Deleted);
- у імені яких присутні неприпустимі символи (Invalid characters).

Таким чином, можливість відновлення даних є вельми важливим напрямом отримання оперативної та доказової інформації при документуванні злочинної діяльності фігурантів. В результаті відновлення комп'ютерної інформації з носіїв, доступ до яких отримано оперативним або слідчим шляхом, можуть бути здобуті відомості, раніше навмисно видалені фігурантом. В даному випадку сам факт такої його поведінки може указувати оперуповноваженому, а згодом слідчому, прокуророві і суду, на обставини, що викривають злочинця і що характеризують суб'єктивну сторону злочину. Крім того, в більшості випадків відновлена інформація має не тільки орієнтуюче значення, але й може бути джерелом доказів у кримінальному судочинстві за умови дотримання законності отримання такої інформації і можливості її легалізації.

## Список використаних джерел


1. Класифікація комп'ютерних злочинів по кодифікатору Генерального Секретаріату Інтерполу [Електронний ресурс]. – Режим доступу: http://www.cyberpol.ru/cybercrime.shtml
2. Конвенція Ради Європи про злочинність у сфорі комп'ютерної інформації ETS № 185, ратифіковано Верховною Радою України із застереженнями і заявами Законом N 2824-IV (2824-15) від 07.09.2005, ВВР, 2006, N 5*6, ст. 71.
3. 15-й, 17-й, 18-й, 42-й, 47-й зводи законів США // Современное право средств массовой информации в США. - М. - 2000, С. 205-223.
4. Закон України «Про основи національної безпеки України» зі змінами та доповненнями - Відомості Верховної Ради України (ВВР), 2003, N 39, ст. 351.
5. Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ // Монографія *І* Д. М. Цехан ; за науковою редакцією О. О. Подобного. - Одеса: Юридична література, 2011.-216 с.
6. Офіційний сайт «Internet Assigned Numbers Authority» (IANA) [Електронний ресурс]. - Режим доступу: http://www.iana.org
7. Сервіс ідентифікації користувача за IP адресою «WHOIS» Інтернет-ресурсу «2IP.RU» [Електронний ресурс]. - Режим доступу: http://2ip.ru/whois.
8. Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов международного сообщества и частного сектора // Группа экспертов для проведения всестороннего исследования киберпреступности / Вена, 25-28 февраля 2013 года: [Электронный ресурс] / UNODC/CCPCJ/EG.4 - 2013. - 21 с. - Режим доступа: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf
9. Конвенція про кіберзлочинність від 23 листоп. 2001 р. [Електронний ресурс].Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_575.
10. Войціховський А.В. Міжнародне співробітництво в боротьбі з кіберзлочинністю / А.В. Войціховський / Науковий журнал «Право і Безпека». - 2011. - №4. [Електронний ресурс]. - Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/pib/2011_4PB–4/PB–4_26.pdf
11. Про ратифікацію Конвенції про кіберзлочинність : закон України від 7 верес. 2005 р. № 2824-IV // Відомості Верховної Ради України. - 2006. - №5-6. - Ст. 71.