Міністерство внутрішніх справ України

ДЕПАРТАМЕНТ КРИМІНАЛЬНОЇ МІЛІЦІЇ У СПРАВАХ ДІТЕЙ

ДНІПРОПЕТРОВСЬКІЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Т.М. Бухтіарова, І.В. Краснобрижий, Є.В. Матвієнко, В.О. Мирошніченко, В.І. Коршун, О.І. Соболь

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

щодо особливостей виявлення фактів розповсюдження дитячої порнографії через мережу Інтернет та документування осіб, що виготовляють та розповсюджують порнографічну продукцію через Інтернет

Дніпропетровськ
2008

ББК 67.9(4УКР)308
М 54

РЕЦЕНЗЕНТИ

Л.М. Карпуков доктор технічних наук, професор, завідувач кафедри захисту інформації Запорізького національного технічного університету;

С.М. Школа кандидат юридичних наук, начальник відділу докторантури та ад'юнктури Дніпропетровського державного університету внутрішніх справ

М 54 Методичні рекомендації щодо особливостей виявлення фактів розповсюдження дитячої порнографії через мережу Інтернет та документування осіб, що виготовляють та розповсюджують порнографічну продукцію через Інтернет/ Т.М. Бухтіарова, І.В. Краснобрижий, Є.В. Матвієнко, В.О. Мірошниченко, В.І. Коршун, О.І. Соболь. – Дніпропетровськ: Дніпропетровський державний університет внутрішніх справ, 2008. – 36 с.

Методичні рекомендації щодо особливостей виявлення фактів розповсюдження дитячої порнографії через мережу Інтернет та документування осіб, що виготовляють та розповсюджують порнографічну продукцію через Інтернет, розроблені на основі вивчення та аналізу вітчизняних і зарубіжних сучасних технічних тенденцій, з урахуванням власних думок та практичних пропозицій фахівців університету.

Методичні рекомендації будуть корисними для науковців, практичних працівників органів внутрішніх справ, курсантів та слухачів.

ЗМІСТ

ВСТУП

Розширення інформаційного обміну із зарубіжними країнами, поява супутникового телебачення, комп'ютерних систем та мереж супроводжується не тільки процесами, які збільшують культурно-комунікативні можливості людини, але і такими, що створюють підґрунтя для поширення порнографічної продукції, яка не в усіх країнах світу є легальною.

У радянський період питання методики розслідування поширення порнографічних предметів у відкритій криміналістичній літературі фактично не висвітлювалися, що не сприяло залученню до її розроблення широкого кола науковців, а відповідно – і появі ґрунтовних наукових досліджень.

Діяльність із розкриття та розслідування злочинів завжди була в центрі уваги вчених у галузі кримінального права, кримінального процесу, криміналістики, юридичної психології та оперативно-розшукової діяльності. Однак такі питання, як: особливості проведення певних слідчих дій при поширенні порнографічних предметів, виготовлених за допомогою сучасної комп'ютерної техніки; сучасні способи вчинення та приховування злочинної діяльності у сфері поширення таких предметів; організовані злочинні групи поширювачів порнографічних предметів; етапи діяльності з виявлення, розкриття й розслідування поширення порнографічних предметів, фази злочинної діяльності у зазначеній сфері не розглядалися взагалі або розглядалися поверхово.

У мережі Інтернет поширюється до 75% всієї дитячої порнопродукції. За даними правоохоронних органів, близько 90% міжнародних пошукових доручень Інтерполу по комп'ютерній злочинності присвячені саме цій проблемі. Світова порнографічна індустрія, знаючи про провальне положення із правовою оцінкою цього виду злочинів у Росії, прагне перемістити свої ресурси дитячої порнографії на територію російської частини Інтернету.

Поширенням дитячої порнографії в Інтернеті з елементами сексуального насильства над дітьми, як правило, займаються добре організовані злочинні міжнародні групи. Кожний дитячий порноресурс Інтернету приносить у середньому дохід близько 30 тис. доларів на місяць. За кожним порноресурсом існує злочинна „тріада": представники організованих злочинних груп, корумповані чиновники, банкіри, що допомагають конвертувати гроші.

Аналіз досліджуваної проблеми свідчить, що ступінь її наукової розробки недостатній, потребує комплексного підходу й більш детального розгляду.

Вказані методичні рекомендації суттєво допоможуть працівникам органів внутрішніх справ у виявленні фактів розповсюдження дитячої порнографії через мережу Інтернет та документуванні осіб, що виготовляють та розповсюджують порнографічну продукцію через Інтернет.

1. Правові засади регулювання кримінальної відповідальності за ввезення, виготовлення, збут і розповсюдження порнографічних предметів за участю неповнолітніх з використанням інформаційного середовища Інтернет

Актуальна нестабільна економічна, соціально-політична ситуація в Україні, поширення явища дитячої безпритульності, бродяжництва, сирітства, моральний занепад суспільства і, як наслідок, безвідповідальна сексуальна поведінка молоді, насильство над дітьми в сім'ї та відсутність належної турботи батьків та опікунів призводить до того, що все більша кількість неповнолітніх у державі стають жертвами сексуальної експлуатації, одним з проявів якої є використання дітей при виготовленні, ввезенні, збуті, розповсюдженні порнографічних предметів.

Новітні комп'ютерні технології, сучасна аудіо- та відеоапаратура дозволяють значно здешевити та спростити виготовлення порнографічної продукції. Сьогоднішні технологічні можливості та ступінь контрольованості інформаційної телекомунікаційної мережі Інтернет, відсутність її територіальних меж, наявність численних способів анонімного розміщення інформації, широка аудиторія користувачів, можливість електронної купівлі-продажу зумовили широке використання віртуального простору представниками порноіндустрії. Такі явища в Україні давно вийшли за межі поодиноких випадків. Сьогодні в мережі Інтернет діють організовані злочинні групи, що розповсюджують порнографічні матеріали за участю неповнолітніх. За даними Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, МВС України, за період 2003–2007 років кількість зареєстрованих злочинів, що передбачені ст. 301 КК України (ввезення, виготовлення, збут і поширення порнографічних предметів) постійно збільшувалася: 2003 р.–235, 2004 р.–281, 2005 р.–366, 2006 р.–571, 2007 р.–811. Упродовж перших трьох місяців 2008 року зареєстровано 238 таких злочинів. Аналізуючи дані показники, можна спрогнозувати, що кількість зареєстрованих вказаних злочинів у цьому році збільшиться.

Серед зазначеної загальної кількості кримінальних справ кількість порушених за ст. 301 КК України кримінальних справ, де потерпілими є діти, у 2002 та 2003 роках становила лише по 3 справи, у 2004 – 6, 2005 – 7, 2006 – 6, 2007 – 5 кримінальних справ [1]. Зрозуміло, що навряд чи ці показники відображають реальний стан проблеми з огляду на очевидну наявність латентних злочинів, про кількість яких можна лише здогадуватися.

Протягом минулого року слідчими підрозділами органів внутрішніх справ було порушено та розслідувалося 7 кримінальних справ, пов'язаних з виготовленням та розповсюдженням дитячої порнографії. У цих справах до кримінальної відповідальності притягнуто 8 осіб, з яких 6 було засу-

джено до різних термінів позбавлення волі, відносно 1 особи кримінальну справу було закрито у зв'язку з амністією на підставі п. 4 ст. 6 КПК України, відносно ще 1 особи справу було направлено до суду в порядку ст. 7–3 КПК України.

Оцінити реальну кількість дітей в Україні, що стали жертвами використання в порноіндустрії, сьогодні досить складно. За спостереженнями працівників правоохоронних органів, сьогодні у переважній більшості випадки використання дітей в порнобізнесі залишаються невідомими.

Серед причин такого стану проблеми є між іншими часті випадки використання неповнолітніх, пов'язані зі злочинами торгівлі людьми та іншої незаконної угоди щодо людини (ст. 149 КК України), коли самі батьки використовують власних дітей для виготовлення порнопродукції або передають іншим особам дітей для виготовлення такої продукції та отримують за це гроші. Також мають місце випадки, коли самі неповнолітні пропонують себе для виготовлення порнографічної продукції через бажання швидко заробити гроші для власних потреб або навіть для сім'ї.

Так, з метою встановлення фактів використання дітей в порнобізнесі, заняття проституцією, вивозом за межі України для їх продажу чи надання послуг інтимного характеру працівниками Департаменту кримінальної міліції у справах дітей МВС України протягом січня – березня 2008 року було перевірено законність діяльності 300 фото- і відеостудій, близько 100 модельних агентств, 1,2 тисячі нічних клубів та розважальних закладів, 400 готелів та кемпінгів, 250 масажних салонів, саун, оздоровчих комплексів, 120 туристичних фірм та бюро з працевлаштування за кордоном, 110 видань у друкованих та електронних ЗМІ, 60 телекомпаній, які здійснюють трансляцію програм кабельним та супутниковим зв'язком, 1,1 тисячі комп'ютерних клубів та Інтернет-кафе, окрім того було проведено близько 8 тисяч рейдів та перевірок, підчас яких перевірено майже 7 тисяч неблагополучних сімей, 600 інтернатних закладів та дитячих будинків, близько 1 тисячі місць реалізації друкованої та електронної фото-відеопродукції [2].

Труднощі при документуванні злочинів, передбачених ст. 301 КК України, полягають насамперед у проблемах виявлення фактичного місця хостингу порносайтів, встановлення фізичного місця розташування техніки, що була використана для їх створення, реєстрації та редагування (оновлення), а також виявлення осіб, причетних до таких дій.

Таким чином, Інтернет являє собою таке середовище, котре дозволяє анонімно здійснювати злочинну діяльність. Злочинні угруповання широко використовують можливості мережі у своїй діяльності. Ними створюються відповідні сайти, web-сторінки, які присвячені секс-індустрії, де розміщена реклама порнографічних предметів з залученням неповнолітніх. Враховуючи величезну кількість користувачів Інтернет, послуги сексуального характеру поставлені на якісно новий рівень. За допомогою Інтернет можна обрати неповнолітнього, переглянути фото, дізнатись іншу інформацію відносно фізичних даних, захоплень, навіть

почути голос. Якщо відповідної анкети не знайшлося, замовник може відправити повідомлення з необхідними параметрами для індивідуального підбору „товару”.

Подальша комп’ютеризація населення України та постійне збільшення користувачів мережі Інтернет за рахунок гіперсексуальних підлітків дозволяє інтенсивно розвиватися порнобізнесу. За оцінками зарубіжних експертів, один „розкручений” порносайт приносить власникам прибуток до 2 млн доларів США на рік [3]. Дитяча порнографія може використовуватися відвідувачами таких сайтів у різних цілях: для створення особистого сексуального збудження та задоволення, в комерційних цілях (наступного продажу матеріалів), для виправдання своєї поведінки, для створення відповідного „авторитету” в певних колах: кримінальних, в середовищі педофілів, для шантажу неповнолітнього, для розбещення чи розпусти, для приниження дитини, отримання викупу тощо.

Належна протидія злочинам, пов’язаним з виготовленням порнографічної продукції за участю неповнолітніх (дітей) та розповсюдженням її через Інтернет, вимагає не лише наявності відповідної матеріальної бази та технічних можливостей вітчизняних правоохоронних органів, високого рівня взаємодії з правоохоронними органами інших держав. Важливим є проведення відповідних наукових досліджень, теоретичних напрацювань щодо удосконалення правових засад регулювання кримінальної відповідальності за ввезення, виготовлення, збут і розповсюдження порнографічних предметів за участю неповнолітніх (дітей) з використанням інформаційного середовища Інтернет, а також накопичення та міжгалузевий аналіз сучасного досвіду іноземних держав щодо нормативного забезпечення, запобігання та способів боротьби з вищеназваними видами сексуальної експлуатації неповнолітніх.

Нормативно-правова база боротьби зі злочинами, що пов’язані з сексуальною експлуатацією неповнолітніх в Україні, побудована на зобов’язаннях, що випливають з міжнародних документів, які ратифіковані українською державою.

Міжнародне законодавство щодо питання дитячої порнографії засноване на Женевській Конвенції „Про боротьбу з поширенням та торгівлею порнографічними виробами” 1923 року, до якої СРСР приєднався у 1935 році.

2 грудня 1949 року резолюцією 317 Генеральної Асамблеї ООН була затверджена Конвенція про боротьбу з торгівлею людьми та з експлуатацією проституції третіми особами, для СРСР вона вступила у силу 9 листопада 1954 року.

7 листопада 1956 року була прийнята Додаткова Конвенція про знищення рабства, работоргівлі та інститутів і звичаїв, подібних рабству, для СРСР вона вступила у силу 30 квітня 1957 року.

15 листопада 2000 року була підписана Конвенція ООН проти транснаціональної організованої злочинності, Україною вона була ратифікована 4 лютого 2004 року. Мета її полягає у сприянні співробітництву в

справі більш ефективного попередження транснаціональної організованої злочинності та боротьби з нею, зокрема щодо збору та аналізу інформації про характер організованої злочинності, підготовки відповідних кадрів, взаємної правової допомоги, спільного розслідування тощо.

З метою посиленого захисту прав дитини 7 вересня 2000 року підписаний Факультативний протокол до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії. Україною даний документ був ратифікований 3 квітня 2003 року. Відповідно до даного документа дитячою порнографією є будь-яке зображення будь-якими засобами дитини, що вчинює реальні чи змодельовані відверто сексуальні дії, або будь-яке зображення статевих органів дитини, головним чином, в сексуальних цілях.

Конвенція № 182 про заборону та негайні заходи щодо ліквідації найгірших форм дитячої праці (ратифікована 5 жовтня 2000 року) заборонила найгірші форми дитячої праці, під якими між іншими визнала і використання, вербування або пропонування дитини для заняття проституцією, виробництва порнографічної продукції чи для порнографічних вистав.

Конвенція про кіберзлочинність, яку було ратифіковано Україною із застереженнями і заявами 7 вересня 2005 року, визначає в ст. 9 „Правопорушення, пов’язані з дитячою порнографією” обов’язок держави-учасниці встановлення належної кримінальної відповідальності за такі умисні діяння, як виготовлення дитячої порнографії з метою її розповсюдження за допомогою комп’ютерних систем, пропонування або надання доступу до дитячої порнографії за допомогою коп’ютерних систем, розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем, здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи, володіння дитячою порнографією у комп’ютерній системі чи на комп’ютерному носії інформації.

Відповідно до тексту документа, поняття „дитяча порнографія” включає в себе порнографічний матеріал, який візуально зображує неповнолітню особу, задіяну у явно сексуальній поведінці, особу, яка виглядає як неповнолітня особа, задіяну у явно сексуальній поведінці; реалістичні зображення неповнолітньої особи, задіяної у явно сексуальній поведінці. Термін „неповнолітня особа” включає в себе усіх осіб до 18 років.

Національне законодавство насамперед в Конституції України офіційно визнає людське життя та гідність найвищою цінністю (ст. 3), гарантує захист дитинства та материнства (ст. 51), державну підтримку сиротам та дітям, позбавленим батьківського піклування (ст. 52 Конституції України).

26 квітня 2001 року був прийнятий Закон України „Про охорону дитинства”, який визначив охорону дитинства загальнонаціональним пріоритетом.

Вітчизняне матеріальне кримінальне право містить інститут кримінальної відповідальності за діяння, пов’язані з дитячою порнографією.

Злочини, пов'язані з дитячою порнографією, посягають насамперед на права дитини насолоджуватися дитинством та на її повноцінне та гідне життя. Комерційна сексуальна експлуатація неповнолітнього може призвести до серйозних наслідків у фізичному, психологічному, духовному, моральному та соціальному розвитку дітей, які можуть зберегтися протягом всього подальшого життя, а часом можуть навіть йому загрожувати.

КК 1960 року передбачав ст. 211 „Ввезення, виготовлення, збут і розповсюдження порнографічних предметів". Ст. 301 КК України 2001 року як наступниця має таку саму назву, але зазнала певних редакційних змін. Так, перелік дій, за які передбачена кримінальна відповідальність, доповнено вказівкою на „перевезення", „інше переміщення", „примушування до участі в їх створенні". Перелік кваліфікуючих ознак доповнено вказівкою на „дії, вчинені щодо... комп'ютерних програм порнографічного характеру", а також „збут неповнолітнім чи розповсюдження серед них творів, зображень або інших предметів порнографічного характеру". Перелік особливо кваліфікуючих ознак доповнено такою, як „примушування неповнолітніх до участі у створенні творів, зображень або кіно- та відеопродукції, комп'ютерних програм порнографічного характеру".

Аналіз ознак складів злочинів, передбачених ст. 301 КК України „Ввезення, виготовлення, збут і розповсюдження порнографічних предметів", можна представити схематично [4]:

Склад злочину	Ознаки складу злочину							
	Діяння	Предмет злочину	Потерпілий від злочину	Наслідки злочину	Місце, час, спосіб, засоби, знаряддя, обставини, ситуація	Суб'єкт злочину	Форма вини	Мотив, мета, емоційний стан
1	2	3	4	5	6	7	8	9
ч. 1. ст. 301	Ввезення в Україну	Твори, зображення або інші предмети порнографічного характеру	-	-	-	-	Прямий умисел	Мета – збут чи розповсюдження
ч. 1. ст. 301	Виготовлення	Твори, зображення або інші предмети порнографічного характеру	-	-	-	-	Прямий умисел	Мета – збут чи розповсюдження
ч. 1. ст. 301	Перевезення чи інше переміщення	Твори, зображення або інші предмети порнографічного	-	-	-	-	Прямий умисел	Мета – збут чи

		характеру						розповсюдження
ч. 1. ст. 301	Збут чи розповсюдження	Твори, зображення або інші предмети порнографічного характеру	-	-	-	-	Прямий умисел	-
ч. 1. ст. 301	Примушування до участі у створенні	Твори, зображення або інші предмети порнографічного характеру	Людина	-	Спосіб – насильницький	-	Прямий умисел	-
ч. 2. ст. 301	Ввезення в Україну, виготовлення, перевезення чи інше переміщення	Кіно- та відеопродукція, комп'ютерні програми порнографічного характеру	-	-	-	-	Прямий умисел	Мета – збут чи розповсюдження
ч. 2. ст. 301	Збут чи розповсюдження	Кіно- та відеопродукція, комп'ютерні програми порнографічного характеру	-	-	-	-	Прямий умисел	-
ч. 2. ст. 301	Примушування до участі у створенні	Кіно- та відеопродукція, комп'ютерні програми порнографічного характеру	Людина	-	Спосіб – насильницький	-	Прямий умисел	-
ч. 2. ст. 301	Збут чи розповсюдження	Кіно- та відеопродукція, комп'ютерні програми порнографічного характеру	-	-		-	Прямий умисел	-
ч. 2. ст. 301	Збут чи розповсюдження	Твори, зображення або інші предмети порнографічного характеру	-	-	Обставини – збут чи розповсюдження серед неповнолітніх	-	Прямий умисел	-
ч. 3. ст. 301	Ввезення в Україну, виготовлення, перевезення чи інше переміщення	Твори, зображення або інші предмети порнографічного характеру	-	-	Обставини – повторно	-	Прямий умисел	Мета – збут чи розповсюдження
ч. 3. ст. 301	Збут чи розповсюдження	Твори, зображення або інші предмети порнографічного характеру	-	-	Обставини – повторно	-	Прямий умисел	-

ч. 3. ст. 301	Примушування до участі у створенні	Твори, зображення або інші предмети порнографічного характеру	Людина	-	Спосіб – насильницький, обставини – повторно	-	Прямий умисел	-
ч. 3. ст. 301	Ввезення в Україну, виготовлення, перевезення чи інше переміщення	Кіно- та відеопродукція, комп'ютерні програми порнографічного характеру	-	-	Обставини – повторно	-	Прямий умисел	Мета – збут чи розповсюдження
ч. 3. ст. 301	Збут чи розповсюдження	Кіно- та відеопродукція, комп'ютерні програми порнографічного характеру	-	-	Обставини – повторно	-	Прямий умисел	-
ч. 3. ст. 301	Примушування до участі у створенні	Кіно- та відеопродукція, комп'ютерні програми порнографічного характеру	Людина	-	Спосіб – насильницький, обставини – повторно	-	Прямий умисел	-
ч. 3. ст. 301	Збут чи розповсюдження	Кіно- та відеопродукція, комп'ютерні програми порнографічного характеру	-	-	Обставини – повторно	-	Прямий умисел	-
ч. 3. ст. 301	Збут чи розповсюдження	Твори, зображення або інші предмети порнографічного характеру	-	-	Обставини – збут чи розповсюдження серед неповнолітніх, обставини – повторно	-	Прямий умисел	-
ч. 3. ст. 301	Ввезення в Україну, виготовлення, перевезення чи інше переміщення	Твори, зображення або інші предмети порнографічного характеру	-	-	Спосіб – за попередньою змовою групою осіб	-	Прямий умисел	Мета – збут чи розповсюдження
ч. 3. ст. 301	Збут чи розповсюдження	Твори, зображення або інші предмети порнографічного характеру	-	-	Спосіб – за попередньою змовою групою осіб	-	Прямий умисел	-
ч. 3. ст. 301	Примушування до участі у створенні	Твори, зображення або інші предмети порнографічного характеру	Людина	-	Спосіб – насильницький, за попередньою змовою групою осіб	-	Прямий умисел	-
ч. 3.	Ввезення в	Кіно- та відеоп-	-	-	Спосіб – за	-	Прямий	Мета

ст. 301	Україну, виготовлення, перевезення чи інше переміщення	родукція, комп'ютерні програми порнографічного характеру			попередньою змовою групою осіб		умисел	– збут чи розповсюдження
ч. 3. ст. 301	Збут чи розповсюдження	Кіно- та відеопродукція, комп'ютерні програми порнографічного характеру	-	-	Спосіб – за попередньою змовою групою осіб	-	Прямий умисел	-
ч. 3. ст. 301	Примушування до участі у створенні	Кіно- та відеопродукція, комп'ютерні програми порнографічного характеру	Людина	-	Спосіб – насильницький, за попередньою змовою групою осіб	-	Прямий умисел	-
ч. 3. ст. 301	Збут чи розповсюдження	Кіно- та відеопродукція, комп'ютерні програми порнографічного характеру	-	-	Спосіб – за попередньою змовою групою осіб	-	Прямий умисел	-
ч. 3. ст. 301	Збут чи розповсюдження	Твори, зображення або інші предмети порнографічного характеру	-	-	Обставини – збут чи розповсюдження серед неповнолітніх, спосіб – за попередньою змовою групою осіб	-	Прямий умисел	-
ч. 3. ст. 301	Примушування до участі у створенні	Твори, зображення, кіно- та відеопродукція, комп'ютерні програми порнографічного характеру	Неповнолітня людина	-	Спосіб – насильницький	-	Прямий умисел	-

Злочини, передбачені ст. 301 КК України „Ввезення, виготовлення, збут і розповсюдження порнографічних предметів", вчинені щодо неповнолітніх потерпілих, слід розмежовувати з суміжними складами, передбаченими ст. 149 КК „Торгівля людьми або інша незаконна угода щодо людини", ст. 150 КК „Експлуатація дітей", ст. 304 КК „Втягнення неповнолітніх у злочинну діяльність", ст. 300 КК України „Ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства та жорстокості", які відрізняються від ст. 301 КК України в основному предметом відповідних злочинів.

Торгівля або здійснення іншої незаконної угоди щодо неповнолітньої особи, а так само вербування, переміщення переховування, передача

або одержання неповнолітньої людини, вчинені з метою використання в порнобізнесі, полягають в кількох видах дій – торгівлі, здійсненні іншої за формою угоди, об'єктом якої є неповнолітня особа, вербуванні, передачі або одержанні неповнолітньої особи. Експлуатація дітей полягає у використанні праці неповнолітнього, що не досяг віку, з якого законодавством про працю дозволене працевлаштування з метою отримання прибутку. Втягнення неповнолітніх у злочинну діяльність полягає у здійсненні психічного чи фізичного впливу на неповнолітнього з метою схилити його до вчинення злочину або участі в ньому чи в інших антигромадських діях, може бути вчинене способом погрози, шантажу, обману, переконання тощо. Відповідальність за ввезення, виготовлення, збут і розповсюдження порнографічних предметів, вчинені щодо неповнолітніх потерпілих, настає у випадку примушування неповнолітніх до участі у створенні творів, зображень або кіно- та відеопродукції, комп'ютерних програм порнографічного характеру.

Злочини, передбачені ч. 2 і ч. 3 ст. 301 КК України слід відмежовувати від адміністративних проступків, передбачених ст. 164-6 КУпАП (демонстрування або розповсюдження фільмів шляхом продажу чи передачі в прокат фільмокопій без державного посвідчення на право розповсюдження і демонстрування фільмів; розповсюдження фільмів шляхом виготовлення фільмокопій без державного посвідчення на право розповсюдження та демонстрування фільмів з метою їх демонстрування, продажу, передачі в прокат); а також передбачених ст. 164-7 КУпАП (розповсюджування і демонстрування фільмів з порушенням умов, передбачених державним посвідченням на право розповсюдження та демонстрування фільмів).

Об'єктом злочинів, передбачених ст. 301 КК, є певні суспільні відносини, які забезпечують основні принципи суспільної моральності у сфері статевих стосунків. Такі дії знаходяться у певному протиріччі з тими моральними засадами, що історично склалися в українському суспільстві, традиціями інтимного спілкування людей, вони завдають шкоду моральному вихованню молоді і шляхом одіозної сексуальної інформації призводять до деформації моральних уявлень і понять про сексуальні відносини між людьми.

Відповідно до Законів України „Про інформацію" від 2.10.1992 р., „Про захист суспільної моралі" від 20.11.2003 р. виробництво та обіг у будь-якій формі продукції порнографічного характеру в Україні заборонені. У той же час виробництво та обіг продукції еротичного характеру є обмеженим, але дозволеним. Критерії віднесення тієї чи іншої продукції до порнографічної чи еротичної встановлює спеціально уповноважений орган виконавчої влади – Міністерство культури і мистецтв. В Україні було створено Національну експертну комісію, яка 20.02.2007 р. затвердила документ під назвою „Критерії віднесення друкованої, аудіовізуальної, електронної та іншої продукції, у тому числі реклами, а також переданих та одержаних по комунікаційних мережах повідомлень та

матеріалів до розряду порнографічної або еротичної продукції". В даному документі Національна експертна комісія визначила формальні та змістові ознаки порнографії, сексологічні критерії порнографії та сексологічні критерії еротики.

Таким чином, предметом злочину, передбаченого ч. 1 ст. 301 КК, є різні друковані чи рукописні твори, живописні зображення, натуралістичні фотографії, фотомонтажні та інші зображення порнографічного характеру. Предметом злочину, передбаченого ч. 2 даної статті, є кінофільми, відеозаписи, магнітофонні записи, комп'ютерні програми, дискети та інші носії інформації порнографічного характеру. На відміну від предметів еротичного характеру, вони за своїм змістом у натуралістичній, цинічній формі відображають статеві органи або натуралістичне чи протиприродне детальне зображення сексуальних відносин. Таким чином, дитяча порнографія може включати фотографії, негативи, слайди, журнали, книги, малюнки, фільми, відеозаписи, комп'ютерні диски та файли. В науковій літературі виділяють дві категорії порнографії: завуальована, що не показує сексуальних стосунків явно, і відкрита порнографія, яка містить зображення дітей, що втягнуті в сексуальні стосунки.

Незважаючи на формальну нормативну визначеність поняття порнографічної продукції, однією з основних причин закриття кримінальних справ відповідної категорії залишається неналежне дослідження слідством питання про те, чи є певні зображення та відеофільми, які розповсюджуються та рекламуються, порнографічною продукцією. Проблема часто полягає в якості проведеної мистецтвознавчої експертизи, наявності у спеціаліста належної освіти в області кіномистецтва та досвіду відповідної роботи.

Наукою кримінального права на підставі аналізу нормативного матеріалу та відповідної слідчої та судової практики розроблені певні ознаки предмета злочинів, передбачених ст. 301 КК:

1) порнографічні предмети мають становити собою річ матеріального світу, це можуть бути книги, фотографії, картини, скульптурні зображення тощо;

2) порнографічні предмети мають у грубій натуралістичній та вульгарній формі зображати статеве життя людей – статеві органи, сексуальні відносини, причому форма такого зображення має бути неприйнятною для суспільної моралі, загальновизначених правил сором'язливості, прихованості відповідних стосунків від сторонніх осіб;

3) призначення порнографічного предмета має полягати в меті збудження статевої пристрасті інших осіб, а також провокування їх статевої агресії. Саме тому законодавцем встановлено, що предметом злочинів, передбачених ст. 301 КК, є лише твори, інші предмети, призначені для збуту чи розповсюдження, а не для власного користування;

4) порнографічні предмети не можуть мати іншого призначення – мистецького, наукового, просвітницького тощо;

5) порнографічні предмети мають сприйматися іншими особами саме як власне порнографічні, що збуджують статеву пристрасть.

З об'єктивної сторони злочини можуть полягати в таких діях щодо порнографічного предмета:

1) ввезення в Україну – такі дії, в результаті яких вказані твори переміщуються через державний або митний кордон на територію України;

2) виготовлення – процеси, які включають в себе як авторство (створення заново чи внесення змін у вже існуючий твір), так і відтворення, розмноження таких творів – друкування, зняття копій, монтаж;

3) збут полягає у оплатній передачі іншій особі, включаючи продаж, обмін, як оплату за виконану роботу чи надані послуги;

4) розповсюдження – безоплатна передача іншим особам, включаючи дарування, передачу у спадок, надання в тимчасове користування;

5) перевезення або інше переміщення – зміна місця знаходження, доставлення з одного місця в інше будь-яким способом.

6) примушування до участі у створенні порнографічних предметів – вплив на інших осіб шляхом застосування фізичного або психічного впливу з метою домогтися того, щоб вони виступили авторами порнографічної продукції (заново написали книгу, сценарій, внесли відповідні зміни до вже існуючих предметів), іншим чином взяли участь у створенні твору (виступили акторами, режисерами, операторами фільму тощо).

Суб'єктивна сторона складається з вини у формі прямого умислу.

Кваліфікуючі та особливо кваліфікуючі обставини зазначені в ч. 2 та ч. 3 ст. 301 і були вказані нами у вищезазначеній схемі.

Вітчизняній історії відомі прецеденти притягнення до кримінальної відповідальності осіб, які лише брали участь у зйомці порнографічних фільмів, позували при виготовленні порнографічних фотознімків та інших предметів порнографічного характеру, вони були притягнуті до кримінальної відповідальності як за пособництво у виготовленні порнографічних предметів (за ст. 19, ст. 211 КК УРСР) [5].

Чинне кримінальне законодавство України не передбачає кримінальної відповідальності за дії, пов'язані з придбанням, зберіганням та користуванням порнографічною продукцією за участю дітей, хоча криміналізація таких діянь, на наш погляд, могла б стати дієвим засобом запобігання вчинення використання дітей у створенні порнографічних предметів. Введення таких діянь до тексту чинного вітчизняного КК відобразило би сучасні європейські тенденції реформування законодавства про відповідальність у сфері сексуальної експлуатації, коли до відповідальності притягується не лише особа, винна в безпосередній сексуальній експлуатації, в тому числі неповнолітніх (дітей), а й особа – замовник послуг, яка формує своєрідний „попит" на „живий товар".

Прикладом актуалізації відповідальності за ввезення, виготовлення, збут і розповсюдження порнографічних предметів, що вчинені щодо неповнолітніх потерпілих, може стати досвід кримінального законодавства Російської Федерації, де законодавцем у 2003 році було розмежовано від-

повідні склади про незаконне розповсюдження порнографічних матеріалів чи предметів, до яких ввійшли незаконне виготовлення з метою розповсюдження або рекламування, розповсюдження, рекламування порнографічних матеріалів або предметів, а також протизаконна торгівля друкованими виданнями, кіно- або відеоматеріалами, зображеннями або іншими предметами порнографічного характеру (ст. 242 КК РФ); та відповідні склади про виготовлення та обіг матеріалів або предметів з порнографічними зображеннями неповнолітніх (ст. 242 -1 КК РФ) [6].

Причому дана спеціальна норма про виготовлення та обіг матеріалів з порнографічними зображеннями неповнолітніх має 2 частини. Ч.1 ст. 242-1 КК РФ разом з виготовленням, зберіганням або переміщенням через Державний кордон РФ з метою розповсюдження, публічної демонстрації або рекламування матеріалів або предметів з порнографічними зображеннями завідомо неповнолітніх, містить відповідний склад злочину, що полягає у залученні завідомо неповнолітніх в якості виконавців для участі в заходах порнографічного характеру особою, що досягла 18 років. Відповідно ч. 2 даної статті містить кваліфікуючі ознаки, такі як вчинення зазначених діянь батьком (матір'ю) або іншою особою – законним опікуном, педагогом або іншим працівником освітнього, виховного, лікувального або іншого закладу, на якого покладено обов'язок здійснювати нагляд за неповнолітнім; вчинення діяння щодо особи, яка завідомо не досягла 14-річного віку; вчинення діяння групою осіб за попередньою змовою або організованою групою.

На наш погляд, поряд з необхідністю удосконалення кримінальної відповідальності за дані діяння, необхідною є розробка комплексної програми протидії факторам, що призводять до поширення та високої латентності відповідних злочинів. Проблема потребує ширшого погляду.

У суспільстві розповсюджуються нові нетрадиційні форми відкритого, масового, публічного розбещення неповнолітніх, надмірної сексуалізації, маргіналізації та криміналізації свідомості та поведінки дітей і підлітків з використанням для цієї мети засобів масової інформації, спеціалізованих еротичних періодичних видань, реклами, відеоіндустрії, сучасних телекомунікаційних засобів, мережі Інтернет, освітніх проектів та інших шляхів інформаційного впливу. Розповсюдження кіно- та відеопродукції, що пропагандує порнографію, сьогодні стало майже звичним явищем. Все це свідчить про необхідність створення активних, адекватних, конкретних заходів реакції комплексної протидії. На науковому рівні – це подальша розробка основних теоретичних положень кримінальної відповідальності за ввезення, виготовлення, збут і розповсюдження порнографічних предметів за участю неповнолітніх з використанням інформаційного середовища Інтернет.

2. Виявлення та документування фактів розповсюдження дитячої порнографії через мережу Інтернет

Ставиться завдання встановити людину, що розмістила порнографічну продукцію. Технічно можливо встановити місце розташування конкретного комп'ютера, з якого інформація була розміщена в мережі.

Існує кілька способів поширення порнографії через Інтернет.

Один з найпоширеніших – це розміщення матеріалів на веб-серверах. Такі сервери можна розділити на дві групи.

Платні сервери. На таких серверах, як правило, потрібна авторизація людини яка розташувала сайт. Адміністрація таких серверів відповідає за зміст сайтів, розміщених на цих серверах.

Анонімні безкоштовні сервери. На таких серверах користувачі можуть розмістити сайти, не вказуючи свої особисті дані.

Кожен комп’ютер у мережі Інтернет має свою унікальну адресу, що складається з чотирьох чисел, які знаходяться в діапазоні від 0 до 255, і розділених крапками. Ось приклад такої адреси:

192.254.55.232

Такі адреси називаються IP-адресами (адресами Інтернет Протоколу), тому що вони забезпечують роботу протоколу IP.

Викладена нижче система адресації базується на IP версії 4, що використовує 32-бітову адресацію. Кожне з чотирьох чисел адреси відповідає восьми бітам інформації. Тому ці числа називаються октетами. Такий адресний простір дозволяє використовувати 255 комбінацій кожної октети, тобто приблизно 4,3 мільярда різних адрес. В даний час Інтернет зіштовхнувся з реальною погрозою недостачі адрес. Тому не дуже давно була розроблена версія IP 6 (має назву „IPng”, чи „Internet Protocol Next Generation”), яка використовує 128-бітну адресацію.

IP-адреса складається з двох частин.

Перша має від одного до трьох чисел ліворуч – позначає мережу, у якій знаходиться комп’ютер, і називається ідентифікатором мережі.

(Інтернет складається з безлічі мереж, кожна з яких має власну адресу.)

Друга має від одного до трьох чисел праворуч – позначає конкретний комп’ютер у мережі і називається ідентифікатором вузла.

Таким чином, ієрархія IP-адрес читається зліва направо, тобто ліворуч розташовуються старші біти, праворуч – молодші (як-то поштова адреса: країна, місто, вулиця, будинок).

Кількість комп’ютерів, що створюють мережі, може бути різною. Будь вона великою чи малою – у будь-якому випадку IP-адреси із загальним ідентифікатором мережі повинно „вистачити” для усіх вузлів. Очевидно, чим більше перше число в IP-адресі (тобто чим більше в ньому бі-

тів), тим більшу кількість адрес можна створити з його використанням. Тому такі числа присутні в адресах великих мереж. Навпаки, менші ідентифікатори мережі говорять про менший розмір мережі.

У залежності від свого розміру мережі поділені на класи. Цих класів чотири – A, B, C, і D, де A позначає найбільші мережі, D – найменший. Розглянемо відмінності, наприклад, мережі класу A від мережі класу C.

Перший октет IP-адреси мережі класу A знаходиться в діапазоні від 1 до 126. Кількість вузлів у такій мережі може досягати 16777214. Ідентифікатори розподіляються в адресі таким способом:

мережа. вузол. вузол. вузол

Перший октет IP-адреси мережі класу C знаходиться у діапазоні від 192 до 233. Кількість вузлів у цьому випадку обмежена 254. Адреса кожного вузла виглядає так:

мережа. мережа. мережа. вузол

Присвоєнням адрес в Інтернет займається організація за назвою InterNIC (Network Information Center). Однак до присвоєння конкретної адреси кожному комп'ютеру не доходить. При реєстрації мережі в Інтернет їй виділяється мережний ідентифікатор у залежності від її класу. Ідентифікація ж вузлів у підмережах мережі здійснюється організацією-власником.

Багато організацій, що мають у своєму розпорядженні великі мережі (наприклад, провайдери послуг Інтернет), іноді „заощаджують” на IP-адресах. Вони резервують меншу їхню кількість, ніж число вузлів у мережі. У цьому випадку кожному вузлу при підключенні виділяється динамічна IP-адреса з тих, котрі вільні в даний момент.

Коли особа підключається до Інтернет, її комп’ютер стає частиною мережі, тому йому повинна бути привласнена унікальна IP-адреса. Отримання IP-адреси здійснюється при кожному підключенні, але ця адреса щораз має нове значення з діапазону динамічних IP-адрес провайдера, через якого здійснюється підключення.

Статичні IP-адреси, як правило, закріплені за тими вузлами Інтернет, що повинні бути присутніми у мережі постійно. Це сервери, призначення яких полягає в тому, щоб обробляти запити користувачів Інтернет.

Хоча комп’ютерам система IP-адресації здається цілком прийнятною у всіх відношеннях, для людини форма подачі інформації представляється не зовсім зручною. Тому для більш легкого уявлення адрес Інтернет була розроблена система доменних імен.

Слово „домен” у перекладі означає „область”, „зона”. Стосовно до Інтернет, домен є віртуальною зоною, до якої належить той чи інший комп’ютер.

Доменне ім’я представляє собою адресу будь-якого ресурсу (інформації) в мережі Інтернет як послідовність слів.

Деякі з них мають змістовне значення, завдяки чому така адреса порівняно легко запам’ятовується.

Адреси Інтернет-ресурсів, представлені таким чином, називають URL-адресами (Uniform Resource Locator), або універсальними покажчиками ресурсу.

Ось типові приклади доменних імен:

www.podrobnosti.ua

www.google.ru

На відміну від IP-адрес, ієрархія доменних імен читається справа наліво. Самий правий сегмент доменного імені являє собою домен верхнього рівня. В даний час Інтернет поділений на домени верхнього рівня по одній з двох ознак: або по географічній, або за ознакою характеру діяльності.

У табл. 1 приведені домени верхнього рівня, що розрізняються за географічною ознакою (сортування зроблене по назвах доменів).

Таблиця 1

.UA	Україна
.RU	Росія
.UK	Великобританія
.US	США
.HN	Гондурас

У списку 1 приведені домени верхнього рівня, що розрізняються за ознакою діяльності сайту.

Список 1

Домени верхнього рівня (сфера діяльності)

com	Комерційні організації
edu	Освітні установи
gov	Урядові організації
mil	Військові організації
net	Організації, що стосуються, як правило,послуг
org	Громадські організації

Оскільки для людини легше сприйняття доменних імен, а для комп’ютера – IP-адрес, між цими двома варіантами запису адреси встановлені однозначні відповідності. Коли комп’ютера дається команда відкрити сторінку, то вводиться визначена URL адреса, це змушує комп’ютер звертатися за довідкою до іншого комп’ютеру, щоб визначити, яка IP-адреса відповідає введеному доменному імені. Цей „довідковий” комп’ютер називається сервером DNS (Domain Name System). DNS – це служба каталогізації доменних імен. Таблиця відповідності доменних імен IP-адресам розміщається на багатьох DNS-серверах, що послідовно опитуються при пошуку того чи іншого значення.

Щоб довідатися IP-адресу сайту, доменне ім’я якого відомо (і взагалі довідатися, чи існує така адреса), можна скористатися програмою Ping (Packet Internet or Inter-Network Groper), що входить у комплект

Windows. Для цього необхідно виконати команду Пуск > Виконати (Start > Run) і набрати наступний рядок:

ping yahoo.com

Замість адреси пошукової системи Yahoo можна ввести адресу будь-якого іншого сайту.

Таким чином можна визначити, за ким зареєстрована та чи інша адреса. Для цього існують програми, узагальнені назвою Whois (що можна приблизно перевести як „Хто є хто"). У комплект Windows така програма не входить, але завантажити її можна з будь-якого сховища програмного забезпечення.

Також зловмисник може скористатися анонімним проксі-сервером або ланцюжком таких серверів. Як правило, на проксі-серверах ведуться протоколи доступу до них. У цьому випадку необхідно витребувати ці протоколи або їх необхідну частину у власників серверів.

Найбільші проблеми виникають із власниками серверів, які є громадянами інших країн.

У боротьбі із комп'ютерною злочинністю та правопорушеннями у сфері комп'ютерних Інтернет-технологій співробітники правоохоронних органів найчастіше зіштовхуються з питаннями:

1. Кому належить той чи інший сайт?

2. Кому належить електронна поштова скринька?

Питання із сайтом вирішується легше з причини того, що він для постійного доступу має статичний адрес та розташований на технічній площадці провайдера, який надає власникові сайту свої ресурси для роботи (це називається послуга хостінгу).

Згідно з описаною вище технологією за допомогою сервісу Whois визначається провайдер, який надає послугу хостінгу. Надалі до провайдера слід звернутися із запитом щодо власників сайту.

Мінімальний рекомендований перелік питань, які має висвітлити провайдер відносно, наприклад, сайту ltd.kiev.ua, такий:

1. Реєстраційні дані (logs) та абонентська інформація про особу, якій надаються послуги хостінгу для сайту ltd.kiev.ua;

2. Адреси, телефонні номери та інші реквізити власника сайту;

3. IP-адреси, які використовувалися для створення цього сайту;

4.IP-адреси, які використовуються для поповнення змісту цього сайту;

5. Інформація щодо змісту цього сайту;

6. Інформація щодо користування зазначеним сайтом.

Для полегшення аналізу отриманої інформації та подальшої роботи з нею необхідно, щоб провайдер до відповіді додав інформацію в електронному вигляді.

Питання 1 і 2 відразу можуть дати відповідь на питання, хто є власником сайту. Але інколи така інформація відсутня у провайдера або сфальсифікована власником сайту (якщо послуга хостінгу у провайдера безкоштовна та не оформляється угодою).

Тоді відповіді на питання 3 і 4 висвітлять інформацію про те, через якого провайдера діяв власник сайту, створюючи та оновлюючи свій сайт, що надасть можливість ідентифікувати його, направивши наступний запит до цього провайдера, але вже по ідентифікації клієнта, що буде описано нижче.

Питання 5 і 6 висвітлюють інформацію про те, що загалом міститься на всьому сайті (бувають приховані, або платні зони), та про осіб, що користувалися цим сайтом для отримання інформації. Якщо у подальшому є задача ідентифікувати таких осіб, то можливо дізнатися, куди було направлено інформацію з сайту.

2. Електронна поштова скринька відрізняється тим, що ім'я користувача відрізняється від доменного ім'я значком @ (комерційна альфа, „собака", „вухо"), наприклад, vovan@ltd.kiev.ua або roma@ukr.net.

При встановленні особи, яка користується відомою адресою, необхідно спочатку встановити за допомогою сервісу Whois провайдера, що надає послуги використання електронної пошти. Далі надсилається запит щодо інформації про користувача електронної поштової скриньки.

Мінімальний рекомендований перелік питань, які повинні бути висвітлені:

1. Адреса, телефонні номери та інші реквізити абонента;
2. IP-адреси, які використовувалися для створення цього облікового запису;
3. IP-адреси, які використовуються для з'єднання з цим обліковим записом;
4. Реєстраційні дані (logs) та абонентська інформація про користувача облікового запису (електронної поштової адреси) roma@ukr.net;
5. Відомості про обліковий запис (електронну поштову адресу), на який пересилається повідомлення після його отримання (робиться операція „Forward");
6. Зміст адресної книги електронної поштової скриньки;
7. Зміст всіх вхідних та вихідних повідомлень.

У цьому випадку зручно, щоб провайдер до відповіді додав інформацію в електронному вигляді.

У випадку використання правопорушником електронної поштової адреси є велика ймовірність, що на перші два питання відповіді у провайдера не буде або інформація буде неправдивою. Це обумовлено тим, що більшість електронних поштових адрес надаються безкоштовно і користувач майже ніколи не заповнює реквізити. Останні три питання дають інформацію про осіб, які можуть надати додаткову інформацію відносно користувача електронної поштової адреси, якого необхідно встановити, інші електронні поштові адреси, які він може використовувати, та його особисті інтереси.

Така інформація тільки опосередковано висвітлює користувача, тому потрібно спиратись на інформацію, яка міститься у відповіді на 3-5 питання.

Тут будуть отримані динамічні IP-адреси інших провайдерів, з яких здійснював свою діяльність користувач електронної поштової адреси, тому дуже важливо знати точний час у відповідності до кожної використаної адреси. Згідно з цією інформацією необхідно за допомогою сервісу Whois встановити провайдера (юридичну особу), який надавав послугу по використанню мережі Інтернет для користувача електронної поштової адреси. Слід направити до нього запит приблизно такої форми:

„...просимо Вас надати інформацію про реквізити клієнта, який здійснював доступ до мережі „Інтернет" з адреси 195.114.131.145 28.02.2002 р. близько 19 години 15 хвилин, а також вказати телефон, з якого здійснювалося з'єднання з мережею, із зазначенням початку та кінця сеансу зв'язку..."

Відповідь на це запитання надасть вам можливість встановити фізичну адресу користувача електронної поштової адреси.

Але якщо електронна поштова адреса створена навмисно для протиправних дій, правопорушник може користуватися нею з комп'ютерних Інтернет-клубів (кафе, орендованих квартир, готелів тощо), тому необхідно буде встановити наступне:

- комп'ютер у внутрішній локальній мережі клубу (кафе або інше місце, де можливо користуватися мережею Internet), з якого правопорушник здійснював свою діяльність;
- який адміністратор закладу був на зміні під час виходу правопорушника до мережі Інтернет;
- осіб з числа інших клієнтів, які в той час знаходились поблизу комп'ютера правопорушника;
- інший обслуговуючий персонал клубу (кафе, готелю тощо), який міг запам'ятати правопорушника (охоронець, бармен, прибиральниця тощо).

Зазначених осіб необхідно опитати та встановити особу (або скласти фоторобот) правопорушника.

У вирішенні питання ідентифікації власника (користувача) сайту або електронної поштової адреси дуже важливий фактор часу, який минув з моменту вчинення правопорушення. Це обумовлено тим, що зазначена в запитах інформація зберігається у провайдера лише деякий нетривалий час, який у більшості випадків не перевищує 1–2 місяці, а інколи складає 5–7 днів. При роботі із будь-яким провайдером слід зазначати, що інформація відносно діяльності клієнта, який представляє оперативний інтерес, в мережі Інтернет має зберігатися якомога довше та бути повнішою.

Після визначення фізичної адреси підозрюваної особи (осіб) наступна слідча дія буде полягати у проведенні обшуку та (у разі необхідності) виїмці знарядь скоєння злочину у вигляді електронних носіїв інформації, які необхідні для подальшого розслідування справи.

Під час вилучення комп'ютера, машинних носіїв та інформації з них виникає ряд загальних проблем, пов'язаних зі специфікою технічних

засобів, що вилучаються. Так, конче необхідно брати до уваги засоби безпеки, які застосовуються злочинцями з метою знищення речових доказів. Вони, наприклад, можуть використати спеціальне обладнання, яке в критичних випадках утворює сильне магнітне поле, що стирає магнітні записи. Дуже поширена історія про хакера Кевіна Мітника, який створив у дверному отворі магнітне поле такої сили, що воно знищувало інформацію з магнітних носіїв при винесенні їх агентами ФБР з його кімнати. Тому завжди треба враховувати, що злочинець має можливість включити до складу програмного забезпечення свого комп'ютера програму, яка примусить комп'ютер періодично вимагати пароль і, якщо декілька секунд правильний пароль не буде введений, дані в комп'ютері будуть автоматично знищені. Власники комп'ютерів встановлюють інколи приховані команди, що знищують чи виконують архівацію з паролем важливої інформації.

Розглянемо таке поняття як доказова електронна інформація. У загальному вигляді доказова електронна інформація – це сукупність інформації, яка зберігається в електронному вигляді на будь-яких типах електронних носіїв та в електронних засобах і має значення для об'єктивного розкриття всіх обставин справи. Особливість цих доказів полягає в тому, що вони не можуть сприйматися безпосередньо, а мають бути інтерпретовані певним чином та проаналізовані за допомогою спеціальних технічних засобів та програмного забезпечення.

Правоохоронні органи в різних країнах утворюють усе більше спеціалізованих підрозділів для збирання та аналізу електронних доказів. Також цю функцію виконують численні лабораторії судової експертизи – як державні, так і приватні.

Дуже часто правоохоронні органи мають справу з комп'ютерами, коли розслідуються і звичайні види кримінальних злочинів: крадіжка, вимагання, шантаж, торгівля наркотиками тощо. Для криміналістів теж усе більш звичним стає пошук та аналіз у комп'ютерних системах інформації, яка може бути використана як доказ при розгляді кримінальної справи в суді. Тому, хоча законодавчі процедури та правила вилучення й оформлення доказів відрізняються в різних країнах, однаковим є те, що визнання комп'ютерних доказів судами – процес важкий і потребує впевненості в тому, що докази були виявлені та вилучені співробітником, який має певні навички та підготовку для цієї діяльності.

Протягом обшуку всі електронні докази, які знаходяться у комп'ютері чи комп'ютерній системі, мають бути зібрані в такий спосіб, щоб вони потім були визнані судом. Світова практика свідчить, що досить часто під тиском представників захисту в суді електронні докази не беруться до уваги. Для того щоб гарантувати їх визнання в якості доказів, необхідно суворо дотримуватися вимог кримінально-процесуального законодавства, а також стандартизованих прийомів та методик їх вилучення.

Розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій, вимагає спеціальних знань. Якщо його буде доручено некваліфікованим особам, то це може створити серйозні проблеми. Тому існує велика потреба у спеціалізованих „комп'ютерних" підрозділах або у кваліфікованих фахівцях.

Комп'ютери, що входять до складу інформаційної системи – це складне обладнання, яке потребує обережного поводження з ним під час роботи на місці події. Слід пам'ятати, що комп'ютери можуть містити в собі велику кількість даних, які належать сторонній особі або організації (наприклад, можуть бути об'єктом інтелектуальної власності). Тому обережність при поводженні з комп'ютером необхідна як з точки зору збереження важливої доказової інформації, так і з точки зору відвернення матеріальних збитків та збереження власності. Саме тому необхідно, щоб з комп'ютером на місці події мала справу дійсно кваліфікована особа.

Справедливим є твердження про те, що не існує такого поняття, як універсальний комп'ютерний експерт. Тому, збираючись на місце події, важливо з'ясувати, з якою технікою і з якою операційною системою доведеться мати справу. Перше, що необхідно встановити, – це тип операційної системи. Не всі комп'ютерні системи однаково розповсюджені, і тут теж можуть виникнути певні проблеми. Спеціаліст з операційної системи MS DOS може не володіти необхідними знаннями для управління машиною з іншою операційною системою, наприклад, Unix або Windows. Але незважаючи на певні труднощі, фахівець має визначитись, чи може він особисто працювати з даною операційною системою, чи залучати іншого фахівця в цій галузі. В останньому випадку дії з обладнанням залучених осіб мають ретельно фіксуватися.

Найбільш простий випадок, коли мова йде про окремий комп'ютер. Але комп'ютери можуть бути пов'язані між собою в комп'ютерні мережі (наприклад, локальні), котрі, у свою чергу, можуть бути об'єднані через глобальні комп'ютерні мережі. Тому не виключена ситуація, що певна важлива інформація (яка може бути використана як доказ) буде передана через мережу в інше місце, не виключено, що й за кордон, а іноді важлива для кримінальної справи інформація може знаходитись на території кількох країн. У такому разі необхідно використати всі можливості (документацію, допити осіб, технічні можливості системи) для встановлення місцезнаходження іншої комп'ютерної системи, куди була передана інформація. Як тільки це буде зроблено, потрібно терміново надіслати запит (з дотриманням встановлених вимог) про надання допомоги (або правової допомоги, якщо така необхідна для виконання поставлених у запиті питань) до компетентного правоохоронного органу відповідної країни (по встановленим офіційним каналам, наприклад, Інтерпол). Саме на цьому етапі виникають найбільші труднощі в організації роботи щодо розслідування злочину, який вчиняється за допомогою комп'ютерних технологій, та кримінального переслідування злочинців.

Сучасні комп'ютерні технології дуже розвинуті та складні, ось чому існує небезпека, що слідство може втратити важливі докази, якщо особи, що ведуть його, не будуть достатньо підготовлені для цього. Необхідно зрозуміти, що реальне фізичне місцезнаходження даних може бути зовсім не в тому місці, як це сприймається на перший погляд. Таким чином, використання локальних і глобальних інформаційних мереж дозволяє приховувати реальне місцезнаходження комп'ютерної інформації не на фізичному жорсткому диску та файловій системі у тому місці, де проводиться обшук і вилучення даних, а в іншому місці або країні.

Особливу цінність при розслідуванні в комп'ютерних мережах мають так звані „логи" – інформація, що міститься в логфайлах (текстова інформація). За допомогою цієї інформації можна, наприклад, встановити рахунок користувача, його ідентифікатор, час трансакції, мережну адресу, телефонний номер, а також, які події відбувалися в системі – що було знищено, змінено, скопійовано, які ресурси були задіяні для цього.

Логи можуть збиратися в комп'ютерних системах на різному рівні: операційній системі, спеціально встановленому програмному забезпеченні (наприклад, програмному аудиті безпеки), окремих модулях баз даних і навіть у деяких прикладних програмах. Фізично ця інформація може знаходитися в різних місцях – від робочої станції і серверу мережі до віддаленого серверу.

До підготовки будь-якої дії, пов'язаної з розслідуванням злочину, що вчиняється за допомогою комп'ютерних технологій (особливо вилучення інформації і комп'ютерного обладнання), доцільно з самого початку залучити фахівця з галузі інформаційних технологій. До початку операції необхідно також мати певну інформацію щодо марки, моделі комп'ютера, операційної системи, периферійних пристроїв, засобів зв'язку та будь-які інші відомості про систему, яка є об'єктом розслідування.

Отримана інформація має бути терміново доведена до фахівця, щоб він мав час для встановлення при потребі додаткового контакту з іншими фахівцями (або його залучення), а також підготувати необхідні спеціальні апаратно-програмні засоби.

Пошук необхідної інформації в комп'ютерній системі може зайняти кілька годин, а іноді й днів. Якщо систему фізично неможливо вилучити й перемістити в інше місце, виникає необхідність копіювати інформацію та комп'ютерні програми на магнітні носії (зробити повні копії окремих жорстких дисків або окремих файлів і директорій). Тому для пошуку, вилучення та копіювання інформації необхідно зарезервувати час.

Магнітні носії, на які передбачається копіювати інформацію, мають бути підготовлені (необхідно впевнитись, що на них нема ніякої інформації). Носії потрібно зберігати у спеціальних упаковках або загортати у чистий папір (не слід використовувати звичайні поліетиленові пакети). Слід пам'ятати, що інформація може бути зіпсована вологістю, температурним впливом або електростатичними (магнітними) полями.

Під час транспортування комп'ютерного обладнання слід поводитися з ним обережно, оскільки інформація на жорсткому диску може бути пошкоджена під час транспортування. Для транспортування великих комп'ютерних систем слід підготувати транспорт та спеціальні упаковки.

Прибувши на місце події (обшуку), необхідно, насамперед, „заморозити" ситуацію: вивести всіх осіб із зони доступу до обладнання, забезпечити неможливість втручання до системи через лінії зв'язку (зокрема через модеми). Не дозволяти нічого змінювати в роботі системи. Система може бути дуже складною, тому, чітко не розібравшись у її конфігурації, не варто приймати жодного рішення.

Окрема увага має приділятися підозрюваній особі, адже можливо, що нею передбачені засоби знищення інформації шляхом натиснення на комп'ютері однієї лише клавіші. Бажано, щоб підозрюваний був присутній при огляді, оскільки саме він може надати найбільш важливу інформацію про систему – паролі, коди доступу, перелік інстальованих програм та місцезнаходження окремих директорій (у тому числі прихованих). Причому його не варто допускати до комп'ютерного обладнання, щоб запобігти спробам знищення комп'ютерних доказів.

Після ретельного обстеження комп'ютерного обладнання робиться його опис у протоколі з наведенням схеми системи. Слід пам'ятати, що помилкове втручання до системи може внести зміни до доказової інформації або призвести до її повної втрати. Крім того, знищення даних або пошкодження обладнання в результаті некваліфікованих дій можуть спричинити матеріальні претензії до організації, яка проводить розслідування.

Доцільно також зробити оглядові та детальні фотографії місця події, при можливості провести аудіо- та відеозапис. Треба враховувати, що окремі компоненти системи можуть знаходитися в інших приміщеннях і, навіть, будівлях або бути добре прихованими. Схованки можуть бути обладнані в стінах будівлі, стелях, на горищах тощо.

Не можна допускати, щоб будь-які особи або непідготовлений персонал вмикали та користувалися вилученим обладнанням. Якщо це можливо, всі дослідження необхідно проводити з участю фахівців спеціальних підрозділів або в судових лабораторіях. Це запобігає випадковим помилкам та забезпечує цілісність вилученої доказової інформації. Всі операції, які здійснюються з системою, мають ретельно фіксуватися.

Перевезення й зберігання комп'ютерної техніки має здійснюватися в умовах, що виключають її пошкодження, в тому числі внаслідок дії магнітних полів, що використовуються для перевірки багажа в аеропортах. При вилученні й перевезенні комп'ютерів не можна ставити їх один на один, розміщувати на них будь-які інші предмети.

Також слід дотримуватися чітких правил поводження з комп'ютерним обладнанням (саме тоді у повній мірі перевіряється ступінь підготовленості співробітників правоохоронних органів).

1. На будь-якому етапі роботи з комп'ютерним обладнанням та доказами комп'ютерного походження, якщо немає впевненості у власних силах, треба дочекатись прибуття експерта або забезпечити участь фахівця.

2. Якщо участь експерта або фахівця неможлива, слід дотримуватися певних вимог і послідовності дій (їх невиконання може призвести до втрати інформації або її доказової сили):

2.1. Не можна користуватися поблизу комп'ютерів радіотелефонами, оскільки вони здатні шкідливо впливати на комп'ютерну систему;

2.2. При охороні комп'ютера не можна дозволяти будь-кому відключати електричне живлення, торкатися клавіатури, змінювати положення комп'ютера або пов'язаного з ним обладнання. Не можна рухати комп'ютер, якщо він підключений. Не можна вимикати принтер до закінчення друкування;

2.3. Треба зафіксувати з'єднання кожної частини комп'ютерної мережі між собою та з іншим обладнанням і сфотографувати його (рис. 1).

Рис. 1. Фотографія з'єднань на задній частині комп'ютера

При роз'єднанні обладнання слід позначити (маркувати) обидва кінці кабелів. Необхідно сфотографувати, як саме комп'ютерне обладнання, так і загальний вигляд кімнати, де знаходилась апаратура, і її підключення.

На цій стадії не можна вимикати або вмикати комп'ютер.

Відключення живлення з метою вилучення обладнання призведе до втрати інформації в тимчасовій пам'яті комп'ютера (RAM), а також може визвати ускладнення з запуском системи в майбутньому, тому що вона може бути захищена паролем.

Якщо екран не світиться, це ще не означає, що комп'ютер обов'язково вимкнений. Можуть бути пошкоджені деякі деталі обладнання, не працювати вентилятор чи бути вимкненим тільки монітор.

2.4. Треба записати у повному обсязі інформацію, яка є на екрані (екранах).

2.5. Слід забезпечити охорону комп'ютерної системи, після чого з'ясувати:

а) Чи підключений комп’ютер до телефонної мережі за допомогою модему;

Якщо комп’ютер підключений через модем, то треба відключити напругу до модему, записати номер використаного телефону.

б) Де знаходиться джерело струму (батареї, джерело безперервного живлення та інше);

в) Необхідно закрити активні програми, після чого можна вимкнути монітор, комп’ютер та відключити напругу.

2.6. Встановити виробника, модель та серійний номер усіх вузлів та операційних систем.

2.7. Від’єднати шнури струму, клавіатури, монітора, модема та принтера.

2.8. При вилученні жорсткого магнітного диска його треба покласти в окремий пакет, опечатати та зазначити номер печатки. Якщо це портативний комп’ютер, то треба вкласти його до конверта, а потім до опечатаного пакета. Не слід самостійно відкривати портативний комп’ютер.

3. При вилученні комп’ютерного обладнання доцільно упакувати в окремі опечатані пакети:

- CPU (кожний окремо);
- портативні комп’ютери;
- дискети;
- окремо змонтовані жорсткі диски;
- носії інформації, які можуть використовуватися разом з комп’ютерами (касети, дискети, лазерні диски).

Варто перевірити, чи були вилучені такі речі:

- монітор;
- клавіатура;
- принтер;
- модем;
- документація та інструкції по експлуатації;
- адаптери до портативних комп’ютерів;
- помічені кабелі та розмикаючи пристрої;
- зразки фірмових та інших бланків комп’ютерного походження;
- роздруковані комп’ютерні тексти, які можуть мати відношення до злочину (вони могли бути знищені на комп’ютері);
- функціональні обов’язки користувачів, адміністратора системи та інформаційної безпеки;
- іншу організаційно-технічну документацію, яка відображає політику безпеки даної установи.

Всі речі та документи мають бути вилучені та описані відповідно до норм чинного кримінально-процесуального законодавства.

4. Необхідно опитати підозрюваних, свідків та всіх причетних до справи осіб.

3. Рекомендації щодо проведення слідчих дій на подальших етапах

Оскільки результати комп'ютерно-технічної експертизи, особливо експертизи програмного забезпечення, прямо залежать від збереження інформації на внутрішніх і зовнішніх магнітних носіях, необхідно при вилученні об'єктів дотримуватись правил, які були вказані вище.

Протягом розслідувань, що пов'язані з комп'ютерами та комп'ютерними системами, найважливішим є уникнути дій, які можуть пошкодити чи змінити наявну інформацію, так чи інакше змінити цілісність вилучених даних. Використання відпрацьованих та перевірених процедур та методик зменшує, але повністю не виключає такої можливості. В ряді випадків окремі дані системи неминуче будуть змінені або переписані в ході проведення досліджень системи, наприклад, зміна тимчасових файлів, поява змін при закритті програм-додатків, на бітовому рівні можуть бути внесені зміни в парольний захист. Особи, які проводять дослідження комп'ютерної системи, мають чітко уявляти всі побічні негативні наслідки проведених з системою операцій та ретельно фіксувати кожен свій крок дослідження, щоб могти пояснити, чому й які зміни відбулися в системі.

Комп'ютери та їх комплектуючі опечатуються шляхом наклеювання на місця з'єднань аркушів паперу із закріпленням їх країв на бокових стінках комп'ютера густим клеєм або клейкою стрічкою, щоб виключити роботу з ними за відсутності власника або експерта. Магнітні носії упаковуються та транспортуються у спеціальних екранованих контейнерах або у стандартних чи інших алюмінієвих футлярах заводського виготовлення, які виключають руйнівний вплив електромагнітних і магнітних полів, направлених випромінювань. Опечатуються тільки контейнери або футляри. Пояснювальні записи можуть наноситись тільки на етикетки для дискет, причому спочатку робиться запис, а потім етикетка наклеюється на призначене для неї місце на дискеті. Якщо на дискеті вже є етикетка з яким-небудь написом, то проставляється тільки порядковий номер, а пояснювальні написи під ним робляться на окремому аркуші, який вкладається в коробку. Неприпустимо приклеювати будь-що безпосередньо до магнітного носія, пропускати через нього нитку, пробивати отвори, робити підписи, помітки, ставити печатки тощо.

У постанові про призначення експертизи вказують серійний номер комп'ютера та його індивідуальні ознаки (конфігурація, колір, написи на корпусі).

Обов'язковою нормою слідчої та експертної практики має стати виготовлення повної копії комп'ютерної системи (її моделі), і всі дослідження проводити з нею, а не з оригіналом. Як правило, такий шлях можливий у будь-якому випадку. Дані, що містяться в системі, можна поділити на три великі категорії:

1) ті, що існують на файловому рівні;

2) ті, що були знищені, але їх можна відновити на файловому рівні;

3) окремі частки даних, що раніше були частками окремих файлів, і які вже неможливо відновити на файловому рівні.

Треба зазначити, що проведення досліджень з цих питань – це процес, який недешево коштує і вимагає значних затрат часу.

Неможливо перерахувати всі методи, обладнання та апаратно-програмне забезпечення, які використовуються для аналізу електронної інформації. З цією метою використовують як загальнодоступні програмні засоби, так і спеціально розроблені програми для правоохоронних органів та експертних лабораторій. Вивчення вилученого матеріалу проводиться, як правило, у спеціалізованих підрозділах, органах судової експертизи, спеціалізованих приватних компаніях, науково-дослідних установах, дослідницьких центрах.

Також треба звернути увагу на великий обсяг інформації, яка за допомогою комп'ютерної техніки може зберігатися або використовуватися зі злочинною метою.

Це насамперед:

- тексти найрізноманітнішого змісту (договори, листи, бланки документів, ділові записи та інші документи);

- графічні файли, в яких зберігаються зображення грошових знаків та інших цінних паперів, бланків, документів (технічних паспортів автотранспорту, посвідчень водія тощо), іншу графічну інформацію;

- електронні таблиці, в яких містяться балансові звіти підприємств, інформація про рух матеріальних цінностей та ін.;

- бази даних, які можуть містити доказову інформацію.

Потрібна інформація може знаходитись у вигляді файлів на носіях інформації персональних комп'ютерів, які являють собою:

- накопичувачі на гнучких магнітних дисках (далі за текстом – ГМД);

- накопичувачі на жорстких магнітних дисках (далі за текстом – ЖМД) двох типів: змінні й незмінні, тобто ті що встановлюються в системний блок, та виносні, які підключаються до спеціального пристрою. Цей пристрій знаходиться поза системним блоком і зв'язаний з ним за допомогою спеціального кабелю та інтерфейсом, або цей же самий пристрій може бути вмонтований у системний блок (виносні накопичувачі вставляються в нього як звичайні ГМД);

- касети з магнітною плівкою, спеціально призначені для резервного архівування та зберігання інформації;

- оптичні диски, які за зовнішнім виглядом дуже схожі на аудіо компакт-диски і бувають двох типів:

1) CD-R, DVD-R – оптичний диск, на який можливо записувати та дописувати інформацію, але без змоги перезапису;

2) CD-RW, DVD-RW – оптичні диски, що дозволяють як записувати, так і стирати інформацію.

Крім того, інформація може знаходитись у оперативній пам'яті комп'ютера, коли він працює. Для збереження цієї інформації необхідно записувати її на дискету (ГМД) або на жорсткий магнітний диск (ЖМД).

Також є можливість встановити дату і час внесення останніх змін у будь-який файл, який цікавить. Особливу увагу слід звернути на інформацію, що міститься в знищених файлах, котру можна відновити і переглянути за допомогою деяких програм (наприклад, з пакету Norton Utilities).

При необхідності можна вилучити дискету, касету з магнітною плівкою або лазерний диск з інформацією, але спочатку необхідно підготувати упаковку для них. Це може бути поліетиленовий пакет, паперовий конверт або коробка з немагнітного матеріалу. На упаковці або бірці, прикріпленій до пакета, необхідно зробити відповідні написи і підписи. Після цього в пакет вкладається вилучений носій інформації. Пакет закривається і опечатується, його треба оберігати від будь-яких механічних, магнітних та теплових впливів.

У випадку вилучення ГМД (ЖМД) необхідно:

1) відключити від струму системний блок;

2) зняти захисний кожух (кришку) з системного блоку;

3) від'єднати ЖМД;

4) запакувати ГМД (ЖМД) відповідно до вищезазначених правил пакування з дотриманням таких вимог обережності:

- не торкатися до магнітного шару на дискетах, касетах з магнітною плівкою;

- не торкатися радіоелементів на платі жорстких магнітних дисків;

- не допускати попадання на робочу поверхню різних мікрооб'єктів;

- не підносити вилучений носій інформації до джерел електромагнітних випромінювань;

- зберігати при температурі не нижче –10 ^{0}C, не вище +52 ^{0}C.

Якщо можна, то необхідно вилучати весь персональний комп'ютер.

З усіх питань, які цікавлять слідчого, орган дізнання, вони мають звертатись за допомогою до спеціаліста або експерта для проведення досліджень.

Перед експертами можна ставити такі питання:

- який склад програмних засобів встановлено на інформаційній системі (ІС) та чи можна за їх допомогою здійснити дії, що інкримінуються обвинуваченому?

- з якими інформаційними ресурсами працював користувач ІС?

- чи не є виявлені файли копіями інформації, що знаходилася в конкретній ІС?

- чи не є виявлені документи документами, які створювалися в конкретній ІС, якщо вони були потім знищені на ІС?

- коли (день, місяць, час, хвилина), ким (кому належить той чи інший пароль доступу), на якій ІС (кому належить робоче місце) проводилася робота на ІС з конкретною інформацією?

- чи не є витік інформації результатом інсталяції спеціалізованого програмного забезпечення?

- чи не заражені вірусом представлені файли (або ІС), і якщо так, то яким саме, яка його дія (знищення, копіювання, модифікація, передача в мережу інформації тощо)?

- чи не містять представлені файли (або ІС) „програмних закладок" і якщо так, то якого саме виду, яка їх дія (знищення, копіювання, модифікація, передача інформації в мережу тощо)?

- чи не є представлені тексти на паперовому носії записами, які потім набиралися конкретним користувачем ІС у конкретному електронному документі?

- чи зазнавала дана комп'ютерна інформація знищення, копіювання, модифікації?

- які правила експлуатації ІС (політика безпеки) існують у даній інформаційній системі та чи були порушені ці правила (робота на ІС у неробочий час, самовільне підключення модему до ІС та інсталяція несанкціонованого програмного забезпечення тощо)?

- чи знаходиться порушення правил експлуатації в причинному зв'язку із знищенням, копіюванням, модифікацією інформації?

- встановити електронні адреси несанкціонованих передач конкретної інформації, хто отримав цю інформацію та яка саме інформація була передана.

У процесі розслідування може статися так, що слідчий чітко знає, який доказ він бажає знайти в комп'ютерній системі: конкретний документ чи угоду. В цьому випадку завдання полегшується і потрібно тільки встановити місцезнаходження цієї інформації в системі. Але ситуація різко змінюється, якщо конкретно невідомо, яка інформація може представляти інтерес для слідства. В цьому випадку особа, що веде розслідування, змушена з допомогою експерта ознайомитись з усіма вилученими матеріалами. Сам експерт не може виконати цю роботу, оскільки в повній мірі не ознайомлений з обставинами справи і не може оцінити доказову силу тієї чи іншої інформації.

Опис можливостей операційних систем по документуванню злочинів

При роботі з ОС Windows створюється велика кількість тимчасової інформації й дуже часто дана інформація довгий час зберігається на жорсткому диску. Це можуть бути дублікати різних документів, тимчасові файли, створені операційною системою або програмним забезпеченням, і.т.п.

Тимчасові файли ОС Windows можна знайти в наступних директоріях:

%SystemRoot%\Temp

(%SystemRoot% – каталог, у який установлена Windows).

%HomeDrive%%HomePath%\Temp

(%HomePath% – Папка Documents and Settings\<ім’я користувача>).

Крім того, тимчасові файли можуть перебувати в поточній директорії.

Або в Unix-Подібних операційних системах,

/tmp або ~/tmp (де ~ - посилання на домашній каталог користувача).

За даними з тимчасових файлів можна визначити яка інформація і якою програмою оброблялася на комп’ютері.

Також існують файли „Кука” (від англ. Cookie – печиво) – короткий фрагмент тексту в протоколі HTTP, що надсилається сервером вебклієнтові (звичайно браузеру). Застосовується для збереження даних на стороні користувача, на практиці звичайно використовується для:

авторизації;

відстеження стану сесії;

ведення статистики про користувачів.

Це означає, що при аналізі „куків” можна з’ясувати, які сторінки відвідувалися користувачем, також там може утримуватися інформація про логіни і паролі користувача.

У браузерах часто ведеться історія відвідування Інтернет-ресурсів. Також ОС Windows зберігає історію документів, що недавно використовувались.

Крім того, існує велика кількість утиліт для відтворення видалених файлів.

Фільтрація небажаних сторінок Інтернет

Основні методи фільтрації

Існує 3 основних методи фільтрації:

- Перевірка вмісту: блокує сторінки, якщо в них міститься набір певних слів;
- Штучний інтелект: поліпшений варіант сканування вмісту;
- Чорний список: блокує сайти на основі списку з категорії

Чорний список.

Для ухвалення рішення про блокування не потрібно завантажувати сторінки. URL фільтр порівнює URL адресу запитуваної сторінки й приймає швидке рішення про блокування.

Перевірка змісту

Перш ніж сторінку перевірити на зміст, вона повинна бути завантажена, що призводить до витрати часу й трафіка. Потім вона порівнюється зі словником і по певному алгоритму приймається рішення про блокування. Недоліком методу є те, що багато сайтів блокуються через помилкове спрацьовування сполучення слів, а сайти із графічним сексуальним змістом і зовсім не перевіряються.

Штучний інтелект

Цей метод так само змушений завантажувати сторінку, що призводить до витрати трафіка й часу для завантаження.

Застосовуються різні варіанти сканування текстового й графічного вмісту. Деякі програми намагаються з'ясувати відсоток оголеної шкіри на фотографіях, що вимагає додаткового навантаження на процесор.

Батьківський контроль в операційній системі Windows

До складу ОС Windows були включені засоби Parental Control (Батьківський контроль). Це дозволяє батькам набагато простіше вирішувати питання контролю за поводженням своїх дітей і їхньою безпекою при роботі на комп'ютері.

Розглянемо функції, розв'язувані за допомогою батьківського контролю.

Обмеження часу, проведеного дитиною за комп'ютером. Можливо визначити час, протягом якого дітям дозволений вхід у систему. Зокрема, визначити дні тижня й дозволені години доступу у відповідний день тижня. Це не дозволить дітям входити в систему протягом певного періоду часу. Якщо в момент закінчення дозволеного періоду дитина працює за комп'ютером, відбувається автоматичний вихід із системи.

Установка заборони на доступ дітей до окремих ігор. Заборона може встановлюватися виходячи із припустимої вікової оцінки, вибору типу змісту або заборони доступу до певних ігор.

Обмеження активності дітей в Інтернеті. Обмежити дітей можна за допомогою установлення кола припустимих веб-вузлів, виходячи з вікової оцінки, заборони або дозволу завантаження файлів, визначення умов фільтрування змісту (тобто ми повинні визначити, який зміст фільтри повинні дозволяти або блокувати). Разом з тим можна дозволити або блокувати доступ до певних веб-вузлів.

Установка заборон на використання дітьми окремих програм. Можна заборонити дітям доступ до певних програм.

Ведення звітів про роботу дитини за комп'ютером.

Веб-фільтр батьківського контролю оцінює вміст веб-вузлів і може блокувати ті з них, зміст яких визначений як небажаний. Включення веб-фільтра дозволить значно зменшити число небажаних вузлів, які змогли б переглядати діти, але, природно, не гарантує стовідсоткового захисту. Тому що небажаність змісту є суб'єктивним критерієм, отже фільтри зможуть блокувати далеко не весь зміст, що ви вважаєте небажаним.

Вибір рівня обмежень для автоматичного блокування вмісту

Існує чотири рівні обмежень для позначення змісту, який варто блокувати:

Високий. Веб-вузли для дітей зі зрозумілим і підходящим для них змістом. На таких вузлах використовується стиль викладу, зрозумілий дітям від 8 до 12 років, а його зміст доступний для дитячого розуміння. Якщо обрано цей рівень, дітям дозволяється переглядати веб-вузли для дітей, а також інші веб-вузли, внесені в список дозволених.

Середній. У цьому випадку проводиться фільтрація веб-вузлів на підставі типу змісту. У цьому випадку дитина отримає доступ до різної інформації в Інтернеті, за винятком небажаного змісту. Щоб довідатися, які веб-вузли дитина відвідувала або намагалася відкрити, варто переглянути звіт про активність в Інтернеті.

Низький. Зміст веб-вузлів не блокується.

Особливий. Даний рівень також передбачає блокування веб-вузлів на підставі типів змісту, але дозволяє робити фільтрацію за додатковими критеріями.

Разом з тим варто відзначити, що можна дозволити або заблокувати окремі вузли, додавши їх у список дозволених веб-вузлів і тих, що блокуються, незалежно від обраного рівня фільтрації.

Вибір типів змісту для блокування

Типи змісту, на підставі яких може здійснюватися блокування веб-вузлів.

Порнографія. Веб-вузол має вміст відверто сексуального характеру, спрямований на поширення статевого потягу.

Для дорослих. Веб-вузол містить інформацію відверто сексуального характеру, що не носить медичного або наукового характеру.

Статеве виховання. Веб-вузол містить інформацію про репродуктивну функцію людини й статевий розвиток, захворювання, що передаються статевим шляхом, контрацепцію, безпечний секс, сексуальність або сексуальну орієнтацію.

Агресивні висловлювання. Веб-вузол пропагує ворожість або агресію стосовно людини або групи людей на підставі приналежності до певної раси, релігії, статі, національності, етнічного походження або інших характеристик; ганьбить інших або виправдовує нерівність на підставі перерахованих вище характеристик або науковим, або іншим загальноприйнятим методом виправдовує агресію, ворожість або наклеп.

Виготовлення бомб. Веб-вузол пропагує або містить інструкції з нанесення фізичної шкоди людям або приватній власності за допомогою зброї, вибухових речовин, розіграшів або інших видів насильства.

Зброя. Веб-вузол продає, висвітлює або описує вогнепальну або холодну зброю, а також предмети бойових мистецтв, або містить інформацію про їхнє використання, аксесуари або модифікації.

Наркотики. Веб-вузол рекламує, пропонує, продає, поставляє, заохочує або іншими способами пропагує незаконне використання, вирощування, виробництво або поширення наркотиків, медичних препаратів, хімічних речовин і рослин, що викликають наркотичне сп’яніння, або атрибутів, пов’язаних із уживанням наркотиків.

Алкоголь. Веб-вузол рекламує або містить пропозиції про продаж алкогольних напоїв або засобів для їхнього виробництва, містить рецепти або інформацію про супутні приналежності або пропагує вживання й сп’яніння алкоголем.

Тютюн. Веб-вузол містить рекламу, пропозиції про продаж або іншими способами пропагує тютюнопаління.

Азартні ігри. Веб-вузол дозволяє користувачам робити ставки й грати на тоталізаторах (у тому числі лотереї) в Інтернеті, одержувати інформацію, сприяння або рекомендації з висновку парі, а також дає інструкції, сприяє або навчає азартним іграм.

Зміст без оцінки. Зміст, що не оцінюється веб-фільтром.

Обмеження доступу дітей до деяких типів змісту в Інтернеті.

Бібліографічні посилання

1. Відомості про зареєстровані злочини, передбачені ст. 149, 161, 300, 301, 304 КК України за період 2003–2004 років, надані Департаментом боротьби зі злочинами, пов'язаними з торгівлею людьми МВС України / Лист від 27.09.2008 № 37/3- 2944.

2. Відомості про кількість кримінальних справ, порушених за ст. 301 КК України, де потерпілими є діти, надані Департаментом кримінальної міліції у справах дітей МВС України / Лист від 22.04.2008 № 13149.

3. Щеглова И.К. Сексуальная эксплуатация несовершеннолетних и пути противодействия / Защита прав и профилактика правонарушений несовершеннолетних. Материалы Международной научно-практической конференции (26–27 августа 2005 года) – М., 2006. – Ч. 2. – С. 183–197.

4. Хавронюк М.І. Довідник з Особливої частини Кримінального кодексу України. – К.: Істина, 2004. – С. 333–335.

5. Кримінальне право України. Судові прецеденти. 1864–2007 рр. / За ред. В.Т. Маляренка. – К.: Освіта України, 2008. – С. 879–880.

6. Федеральный Закон от 8 декабря 2003 года № 162 - ФЗ // Собрание законодательства Российской Федерации. – 2003. – № 50. – С. 48.