УДК 004.738.1:026.6:002.1:004.056

Антон Вітушко,
заввідділу програмно-комунікаційних технологій СІАЗ НБУВ

ПРОБЛЕМА ВИКОРИСТАННЯ В БІБЛІОТЕЧНОМУ ІНФОРМАЦІЙНОМУ ВИРОБНИЦТВІ СОЦІАЛЬНИХ МЕРЕЖ З ТОЧКИ ЗОРУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті порушується питання загроз, які несуть у собі соціальні мережі. Наводяться основні типи існуючих методів, які використовують кіберзлочинці. Розглядаються шляхи вирішення проблем інформаційної безпеки під час використання соціальних мереж у бібліотечному інформаційно-аналітичному виробництві.

Ключові слова: соціальні мережі, кіберзлочинці, акаунти, таргетована реклама, шкідливий код, спам, методи соціальної інженерії, фішинг, фармінг, бот-нет, DDoS-атаки.

Нині соціальні мережі є середовищем, у якому ми не тільки розважаємося, але й працюємо. Співробітники бібліотек також використовують їх для отримання відгуків стосовно своєї роботи, співробітництва з колегами. Бібліотечним установам соціальні мережі необхідні як середовище для спілкування з читачами, для ефективного розвитку продуктивності праці, інноваційного розвитку.

Початок сучасної теорії соціальних мереж поклали в 1951 р. Р. Соломонофф і А. Рапопорт. Поняття соціальна мережа ввів у 1954 р. соціолог Д. Барнс [3]. На його думку, соціальна мережа – це соціальна структура, що складається з групи вузлів, якими є соціальні об'єкти (люди або організації), і зв'язків між ними (соціальних взаємовідносин). Д. Уоттс і С. Строгач розвинули теорію соціальних мереж і ввели поняття коефіцієнта кластеризації (clustering coefficient) – ступеня близькості між неоднорідними групами.

У 1995 р. Р. Конрадом була створена перша соціальна мережа в сучасному розумінні – Classmates.com. З цієї концепції розпочався швидкий розвиток соціальних мереж в Інтернеті.

Соціальні мережі, форуми, блоги – це середовище з практично миттєвою швидкістю поширення інформації і досить сильним ефектом

пам'яті (вміст багатьох соціальних ресурсів індексується і є доступним з пошукових систем).

Але ті характеристики, які роблять соціальні мережі привабливим середовищем для інформаційної роботи, несуть у собі значні ризики з точки зору інформаційної безпеки: загрозу цілісності інформації через її доступність, а отже – можливість крадіжки, фальсифікації, отримання нецензурної інформації.

Крім того, як стверджують фахівці, більшість людей використовує один пароль на багато сервісів, тому, «взламавши» пароль від соціальної мережі, зловмисник, у більшості випадків, отримує пароль від електронної пошти, облікового запису на робочому ПК, службової бази даних. Якщо раніше для отримання адреси приватної електронної пошти зловмисникам потрібно було витратити багато зусиль, то сьогодні достатньо знати лише прізвище, ім'я і місце роботи. А ці дані досить легко знайти в соцмережах.

Соцмережі розширюють свої можливості та послуги, а отже – дедалі більше відкривають кожного з учасників зовнішньому світові. Сьогодні в ЗМІ зустрічається чимало повідомлень стосовно випадків витоку персональних даних, акаунти користувачів легко «взламуються», у адміністрації мереж є доступ до будь-якої інформації. Тому останнім часом тема інформаційної безпеки в соціальних мережах привертає чимало уваги.

Зокрема, одним з варіантів використання персональних даних без дозволу користувача є стандартні для майже всіх мереж внутрішні механізми для показу таргетованої реклами, підбору потенційних знайомих або потенційно цікавого контенту. Ці механізми діють за принципом збирання та аналізу персональних даних, які використовуються з комерційною метою. Причому це робиться відкрито, ніхто цього не приховує.

Чимало проблем створюють користувачам і випадки витоку персональних даних з вини мережі. У 2011 р. стався витік персональних даних (можливо, і платіжних даних) 77 млн користувачів ігрової мережі PlayStation Network [1]. На думку фахівців, наслідки цього інциденту поки недостатньо проаналізовані, і ймовірно, що більшість подібних ситуацій приховується від громадськості власниками соцмереж.

Ще більш серйозні проблеми може викликати «взламування» окремих акаунтів і отримання доступу до персональної інформації певного користувача. Сьогодні зробити це не складно навіть для будь-якої людини, яка вміє використовувати соціальну інженерію. Крім того, в Інтернеті існує спеціальна послуга зі «взламування», вартість якої близько 20 дол. Мотивація зловмисників може бути різною: від отримання інформації

про певну людину з метою компроментації шляхом внесення змін до цієї інформації до отримання інформації про посадовців певної організації з метою промислового шпигунства.

Але найбільша загроза полягає в тому, що доступ до всієї персональної інформації в соціальних мережах є у досить великої кількості людей, і вони можуть у будь-який момент її проглядати, навіть у тому випадку, якщо людина видалила щось з мережі. Зокрема, це співробітники соціальної мережі, у яких є доступ до баз даних, та спеціальні інструменти входження в акаунти користувачів (наприклад, спеціальний майстер-пароль у Facebook). І це цілком логічно: робота співробітників соціальних мереж полягає у керуванні ними, що неможливо без вільного доступу до всіх ресурсів мереж.

Тому останнім часом активні користувачі соціальних мереж ретельніше аналізують інформацію, яку оприлюднюють в Інтернеті; видаляють компромат. Проте такий крок може не дати практичного результату: часто інформація зберігається на серверах компанії і може бути використана в будь-який момент.

Загалом в соціальних мережах спостерігається і цілий спектр інших загроз, враховуючи шкідливий код і спам, використання методів соціальної інженерії на базі фітингу (злочинці можуть використовувати їх як для розповсюдження зловмисного коду, так і для розвідки, щоб потім здійснити спрямовану атаку).

Оскільки соціальні мережі є квінтесенцією сучасних веб-технологій, вони також об'єднують у собі всі загрози, властиві Інтернету. Якщо в організації для співробітників не заборонений доступ до Інтернету або його ресурси використовуються в процесі роботи, вона підпадає під інформаційні ризики, враховуючи шкідливий код, спам, фішинг і т. ін. Утім, соціальні мережі з гарною репутацією стежать за тим, що публікується на їх сторінках, і прагнуть самостійно боротися з вірусами і шкідливим кодом, тому підвищення ризику, пов'язаного з класичними зовнішніми загрозами є незначним.

Дещо інакше виглядає ситуація із захистом від внутрішніх загроз і пов'язаних з ними витоків конфіденційної інформації. Як і у випадку із зовнішніми загрозами, використання соцмереж підвищує такі ризики: неуважний або нелояльний співробітник може опублікувати там інформацію обмеженого доступу. Окрім того, у мережах зловмисники можуть неформально спілкуватися із співробітниками організації на будь-які теми, отже, з'являється набагато більше можливостей для отримання конфіденційної інформації.

Поширена в соцмережах пропозиція «дружби» від невідомих або маловідомих людей може призвести до неприємних наслідків. Рівень довіри до тих, хто перебуває в списку «друзів», апріорі вищий, аніж до випадкових людей. Поширений в соцмережах доброзичливий тон спілкування створює помилкове враження, що навколо тільки друзі, з якими можна ділитися будь-якою інформацією.

Чимало користувачів сприймають акаунти в соціальних мережах як особисті електронні щоденники, де можна фіксувати свої думки, ділитися спогадами, описувати свої стосунки з друзями і колегами. Та на відміну від паперових щоденників, інформацією соціальних мереж може скористатися будь-хто і будь-коли.

Дослідники США, Великобританії, Японії та Німеччині відзначають, що кількість відвідин соціальних мереж з робочих місць сьогодні швидко зростає [2]. Більшість респондентів визнає, що вони присвячують спілкуванню в соцмережах значну частину свого робочого дня. У такій ситуації було б дивним, якби кіберзлочинці не перетворювали соцмережі на джерело інформації, яка може принести матеріальну вигоду.

Зокрема, Wall Street Journal 18 жовтня 2010 р. опублікувала новину про те, що деякі популярні додатки Facebook автоматично пересилали ID-номери користувачів брокерській конторі, яка, у свою чергу, передавала ці дані рекламним компаніям [2].

З одного боку, ID-номер ніякої персональної інформації в собі не несе. З іншої – вставивши номер в адресний рядок Facebook, будь-хто може потрапити на сторінку користувача та отримати потрібну інформацію.

На думку фахівців, причиною такого явища є не самі мережі, а небажання користувачів уважно прочитати всю інформацію до пропонованих йому додатків і налаштувань приватності.

Зокрема злочинців завжди цікавить інформація, яка – за допомогою стандартних запитань (дівоче прізвище матері і т. ін.) допомагає відновити пароль користувача (особливо до системи інтернет-банкінгу). Враховуючи той факт, що деякі користувачі докладно висвітлюють у соцмережах приватне й професійне життя, на них легко можуть вийти шантажисти.

Основним інструментом кіберзлочинців у соцмережах стають прийоми соціального інжинірингу [5], що експлуатують недосвідченість,

[5] На думку фахівців аналітичної фірми Gartner, соціальний інжиніринг – це маніпулювання людьми, а не машинами, з метою проникнення в захищені інформаційні системи підприємства або споживача (докладніше див.: http://www.algonet.ru/?ID=459597).

неуважність та необережність користувачів. Тому людський фактор є ключовим у забезпеченні інформаційної безпеки.

Слід також відзначити, що сучасні кіберзлочинці не обмежуються крадіжками персональної інформації користувачів. Часто головною метою їхньої діяльності є запуск ще більших атак через сторінку жертви на соціальному сайті, підключення комп'ютера жертви до бот-нету для масових розсилок спаму, участі в DDoS-атаках. Соціальні мережі притягують кіберзлочинців перспективою значної кількості потенційних жертв, за рахунок яких вони можуть надати чимало сервісів. А це – можливість заробити значні гроші.

Загрози, які несуть у собі соціальні мережі, можна поділити на такі основні типи.

Перший тип загроз. Введення в оману – основний «компонент» соціальної інженерії, що складається з низки технологій: видавання себе за іншу особу, відволікання уваги, нагнітання психологічного напруження і т. ін. Кінцева мета дій кіберзлочинців дуже різноманітна.

Зокрема, претекстінг – дія, відпрацьована за наперед складеним сценарієм (претексту), у результаті якої жертва повинна видати певну інформацію, або вчинити певну дію. Часто ця технологія вимагає певних попередніх досліджень (наприклад, персоналізації: дата народження, сума останнього рахунку та ін.) для того, щоб забезпечити довіру жертви.

Ще однією технологією є так званий маскарад, або підміна особи, коли кіберзлочинець приховує свої дії прізвищами друзів або прикривається в соцмережі фотографіями знайомих. Сценарій подібного маскараду можливий і проти певної організації або закладу. Його результатом може стати організація «чорного піару».

Цікавою технологією інтернет-шахрайства є фішинг (від англ. Phishing – рибний лов), метою якого є отримання доступу до конфіденційних даних користувачів – логінів та паролів. Зокрема звичайним прийомом є лист або повідомлення від адміністрації популярного сервісу з пропозицією проголосувати за фотографію, внести платіж за певні послуги. Лист або повідомленя містить посилання на фішинговий сайт, який ззовні не відрізняється від оригіналу. Після того як користувач заходить на нього він, як правило, вводить свої персональні дані, що і є метою злочинців.

Можливий і інший варіант розвитку подій: коли користувач заходить на фішинговий сайт спеціальний скрипт визначає версію операційної системи та браузера жертви. Одержані дані дають можливість визначити

експлойт, за допомогою якого відбувається правка файлу HOSTS, завантажується та активізується троян, який може викрасти всі дані та паролі.

Небезпечнішим за фішинг є фармінг (від англ. pharming, farming – сільське господарство), який з'явився в результаті еволюції фішингу. Фармінг – це замасковане перенаправлення користувача-жертви на помилкову IP-адресу. Яка між ними відмінність? Якщо у випадку з фішингом жертва потрапляє на сайт з іншим ім'ям, то у випадку з фармінгом, ім'я залишається незмінним – змінюється тільки IP-адреса серверу. Навіть досвічений користувач може не знати, що він потрапив на фармінг-сайт, якщо у нього немає можливості проглядати IP-адреси сайтів і порівнювати їх.

Останнім часом особливої популярності у користувачів набули сервіси для скорочення довжини URL, але вони дають змогу замаскувати адресу небажаного сайту під коротким посиланням. Насправді домен лише перенаправляє відвідувача. Сьогодні йде активна боротьба з цими ризиками – сервіси скорочення URL застосовують поліпшені механізми детектування спама та інших загроз. Проте для користувачів соціальних мереж загроза залишається – принадні пропозиції від відомих контактів, які були «взламані» кіберзлочинцями, часто призводять до завантаження вірусних програм.

Другий тип загроз пов'язаний із «взламуванням» призначених для користувача записів соціальних ресурсів. За допомогою таких дій зловмисник може потрапити в соцмережу (від імені особи, яка представляє в ній організацію або бренд), розіслати за її списком друзів фішингове повідомлення і мотивувати одержувачів до певних негативних дій – зокрема, пройти по вказаному посиланню та запустити шкідливий код.

Значну загрозу містить у собі звичка використовувати однакові імена користувачів і паролі в корпоративній мережі та в зовнішніх соціальних ресурсах. «Взламування» такого запису, призначеного для користувача соцмережі, значно підвищує ризик проникнення до ресурсів організації від імені одного із її співробітників. Крім того, зловмисник, який має реєстраційні дані жертви, може використовувати їх для розсилання програми для крадіжки паролів на комп'ютери партнерів організації. У результаті кількість комп'ютерів-жертв швидко зростатиме.

Згідно з дослідженням фахівців Массачусетського університету, середньостатичному хакеру для «взламування» пароля потрібно 30–60 хв (залежно від досвіду). Складні ж паролі потребують спеціальних програм, які містять словники з паролями. Навіть перший «черв'як», написаний у 1988 р., умів підбирати паролі за словником [4].

Окремо слід сказати про Cookies – невеликий фрагмент службової інфор-

мації, що розміщується веб-сервером на комп'ютері користувача. Він застосовується для збереження даних, специфічних для даного користувача, використовуються веб-сервером для різних цілей. Може зберігати будь-які призначені для користувача налаштування, зокрема ключ сесії (без пароля), зашифрований пароль, комбінацію із зашифрованого пароля та логіна. Все це є цінною інформацією для злочинців. Тому його можуть:

1. Вкрасти. Простіше всього це зробити, маючи доступ до призначеного для користувача комп'ютера (через інтернет-з'єднання значно складніше). Крадіжка cookies через інтернет-з'єднання дає хакеру доступ до акаунта користувача, пароль від нього, а також багато іншої цінної інформації.

2. Підмінити. Підміна Cookies відбувається безпосередньо перед відправленням на сервер.

Найпростіше всього Cookies вкрасти в місцях з вільним доступом до Wi-Fi. Найсерйозніший захист Cookies надають захищені канали (HTTPS-сесія плюс атрибут SECURE у Cookies).

Третій тип загроз. Оскільки соціальні мережі є веб-додатками, хакери можуть використовувати їх з метою організації атак на браузери. Інструментами для таких атак можуть слугувати троянські додатки, фальшиві антивіруси, соціальні «черв'яки». Їх головна мета – проникнення до інформаційної системи відвідувача соціальної мережі та закріплення в ній. Для захисту використовуються такі традиційні засоби, як антивірусні програми, які працюють у режимі реального часу і блокують завантаження шкідливих кодів.

Четвертий тип загроз. Розсилання за допомогою отриманих у результаті «взламування» сторінок у соціальних мережах персональних даних спаму (англ. spam) – реклами або іншого виду повідомлень особам, які не висловлювали бажання їх отримувати. Легальність масової розсилки деяких видів повідомлень, для яких не потрібна згода одержувачів, може бути закріплена в законодавстві країни. Наприклад, це можуть бути повідомлення про стихійні лиха.

Найпоширенішим видом спаму є реклама. Деякі компанії, які займаються легальним бізнесом, рекламують свої товари або послуги за допомогою спама. Часто вони замовляють розсилку компаніям (або особам), які на цьому спеціалізуються. Привабливість такої реклами полягає в її низькій вартості і великому обсязі потенційних клієнтів.

У зв'язку з посиленням у світі антиспамового законодавства частка легальних товарів і послуг у загальному обсязі спаму останнім часом скорочується.

За допомогою спаму часто рекламують продукцію, про яку не можна повідомити іншими способами. Зокрема, порнографію, контрафактні товари, незаконно отриману закриту інформацію (бази даних), контрафактне програмне забезпечення.

Заборонена законодавством про рекламу інформація, зокрема та, що підриває репутацію конкурентів та їх продукції і послуг, також може розповсюджуватися за допомогою спаму.

Інші види спаму:

– розповсюдження політичної пропаганди;

– масова розсилка для виведення поштової системи з ладу (DDoS-атака);

– масова розсилка від імені певної особи, для того, щоб викликати до неї негативне ставлення;

– розсилка листів, що містять жалісну історію (як правило, про хворого) з інформацією про те, що за кожну пересилку листа інтернет-провайдер нібито виплатить йому певну суму грошей «на лікування». Метою такої розсилки є збір електронних адрес: після численних пересилок «усім знайомим» у тексті такого листа часто містяться e-mail усіх, кому він був надісланий раніше.

П'ятий тип загроз. Загрозою, що відноситься до економічної безпеки організації, є компрометуюча поведінка її співробітників у соцмережах: епатажні публікації можуть завдати певної шкоди репутації організації.

Шостий тип загроз також належить до економічної безпеки організації – зростання трафіку, особливо при прогляданні відеоджерел. Щоб зменшити ці витрати, можна обмежити доступ до відеотрафіку для тих співробітників, посадові функції яких його не передбачають.

Розглянемо варіанти існуючого захисту від загроз, що несуть у собі соціальні мережі.

Варіант перший: блокування доступу на сайти даної категорії. У великих компаніях саме так і роблять, адже соціальні мережі – це втрата робочого часу й зниження продуктивності. Проте сьогодні більшість необхідних професійних контактів проходить саме через соцмережі. До того ж це необхідний інструмент у руках маркетологів, фахівців із зв'язків із громадськістю, з підбору персоналу, аналітиків, бібліотекарів.

Варіант другий: контроль над користуванням сайтами даної категорії. Такий варіант є більш прийнятним для організацій, для яких Facebook і Twitter є майданчиками активної професійної діяльності. Але в цьому випадку постає питання про потенційну загрозу витоку інформації через соціальні мережі.

Що б захиститися від цього, у першу чергу треба виявити інформацію, яка є конфіденційною. Контролюючи всі канали передачі інформації всередині організації, можна контролювати інформаційні потоки в соцмережах, на форумах та блогах.

Проаналізуємо найпоширеніші причини заборони користування соціальними мережами на роботі:

1. Соціальні мережі сприяють витоку інформації. Разом з тим, конфіденційну інформацію можна успішно поширювати і через електронну пошту, телефон, побутові розмови.

2. На соціальні мережі витрачається робочий час. Але це проблема не користування соціальними мережами, а мотивації співробітників. Робочий час можна витрачати і на читання новин.

3. Соціальні мережі – джерело вірусів та інших шкідливих програм. Але вірус можна прийняти електронною поштою або з диску з піратським програмним забезпеченням.

На думку багатьох експертів, заборона на спілкування в соцмережах несе в собі не лише загрозу, а й втрачену можливість використовувати в роботі могутній інструмент комунікації, який можна успішно використовувати для інновацій у роботі. У багатьох організаціях вже працюють фахівці, у сферу обов'язків яких входить просування продуктів і послуг через соціальні мережі. Зокрема, досвід такої роботи мають співробітники СІАЗ та НЮБ НБУВ Т. Гранчак, Л. Чуприна, І. Гах. Але доступ до соціальних мереж потрібно контролювати. У першу чергу, через навчання співробітників основним правилам безпечного використання цього каналу комунікації.

Існують і ситуації, за яких необхідно забороняти доступ до соціальних мереж. Зокрема, якщо:

– існує корпоративна необхідність ізолювання працівника від віртуального світу;

– тимчасово або постійно відсутній контроль і керування доступом до соціальних мереж;

– ефективність праці співробітників знизилась.

І якщо перша ситуація може скластися через об'єктивні обставини і повинна трансформуватися в перманентну вимогу, то дві інші повинні сприйматися як тимчасові, викликані упущеннями в питаннях управління і технічної оснащеності.

Постійна заборона використання соціальних мереж на робочому місці не допоможе розв'язати проблему витоку конфіденційних даних, тому що блокування одного з каналів передачі інформації може спровокувати

пошук альтернативних шляхів передачі даних. Контроль користування соцмережами дає можливість не лише виявити інсайдера, а й зрозуміти настрої в колективі.

Багато в чому бажання організацій заборонити, а не контролювати соціальні мережі обумовлюється нерозумінням технічних принципів їх контролю і перспектив роботи з ними.

Останнім часом тема інформаційної безпеки й приватності в соціальних мережах привертає увагу багатьох фахівців. Слід зазначити, що сьогодні компанії, які займаються розробкою продуктів для захисту корпоративних мереж, вже вміють цілеспрямовано фільтрувати веб-додатки, з яких складаються соціальні мережі. Такі продукти дають змогу заборонити окремі додатки, групи додатків або окремі функції соціальних мереж.

Вже існують адекватні засоби захисту, що дають можливість знизити ризик використання соцмереж до прийнятного рівня:

1. Для захисту від витоків інформації можна використовувати сучасні DLP-системи і технології репутацій, які інтегровані в різні антивірусні продукти.

2. У частині технічних засобів протидії шкідливому ПО – комплексні засоби моніторингу, аналізу й фільтрації вхідного і витікаючого трафіку на рівні шлюзів, а також засобу аналізу поведінки додатків і мережних комунікацій.

3. У частині керування доступом до потенційно небезпечного середовища – диверсифіковані внутрішньокорпоративні політики «білих списків» і фільтрації контенту для різних груп користувачів. Суть їх полягає не в розподілі привілеїв користування засобами обміну миттєвими повідомленнями, а в оптимізації ризиків.

Зокрема, для кожної групи користувачів створюється специфічний «білий список», наприклад, за наслідками оцінки потенційної небезпеки ресурсів з погляду існуючої веб-репутації, або наявності-відсутності сертифікату SSL, або за певним профілем контентної фільтрації. Мова йде не про банальний перелік ресурсів, дозволених до використання. Відповідно налаштовуються і засоби безпеки для групи користувачів. Для тих, хто повинен працювати в потенційно більш небезпечному середовищі, заборони будуть жорсткішими.

Існуючі методи боротьби на корпоративному рівні будуть ефективні за умови, що розробник засобів боротьби із загрозами регулярно оновлює свої рішення на основі нових загроз, що поширюються через соцмережі, і засоби їх мінімізації.

В організаціях, яким не потрібно сильно обмежувати своїх співробіт-

ників у використанні Інтернету, політика інформаційної безпеки стосовно соцмереж майже не відрізняється від політики використання інших інтернет-ресурсів. У цих правилах потрібно вказати, яку інформацію можна публікувати в соціальних мережах, а яку – ні, яким працівником дозволено користуватися соцмережами, а яким – ні. Загалом для політики інформаційної безпеки соціальні мережі є такими ж інтернет-ресурсами, як і форуми, блоги, сервери безкоштовної електронної пошти.

Крім того, необхідно проводити адекватну роз'яснювальну роботу серед персоналу стосовно безпечної поведінки в сучасному інформаційному просторі.

Отже, реалізація заходів з інформаційної безпеки стосовно соцмереж – це великий обсяг роботи не лише з персоналом (створення й доведення до уваги співробітників локальних нормативних актів, регламентів або інструкцій, упровадження режиму комерційної таємниці, великого комплексу організаційно-методичних заходів), а й значний комплекс організаційно-технічних робіт.

Про важливість такої роботи свідчить і той факт, що за допомогою соцмереж сьогодні моделюються не лише персональні або корпоративні витоки інформації, а й соціальні конфлікти різного рівня. Тому питання про контроль за діями в соціальних мережах дедалі більше цікавить державні органи. Не виключено, що в найближчі роки питання відповідальності за протиправні дії в соцмережах буде вирішуватись на законодавчому рівні.

Список використаних джерел

1. *Андреев Э. М.* Социальные проблемы интеллектуальной уязвимости и информационной безопасности / Э. М. Андреев, А. В. Миронов // Социально-гуманитарные знания. – 2000. – № 4. – С. 169–180.

2. *Гольфред Я. А.* Философия и история науки управления [Электронный ресурс] / Я. А. Гольфред // Философия и история науки управления. – Режим доступа: http://afield.org.ua/book/t_upr.html (12.04.2011) – Загл. с экрана.

3. *О'Рейли Т.* Что такое Веб 2.0 [Элетронный ресурс] / О'Рейли Тим // Компьютерра online. – Режим доступа: http://www.computerra.ru/think/234100/ (12.04.2011). – Загл. с экрана.

4. *Попов В. Б.* Основы информационной безопасности. Информационные технологии и право / В. Б. Попов // Основы компьютерных технологий. – 2002. – С. 175–187.