**УДК 004.056**

**Н.П. Кухарська[1], В.М. Кухарський[2]**
[1]Львівський державний університет безпеки життєдіяльності,
кафедра управління інформаційною безпекою,
[2]Львівський національний університет імені Івана Франка,
кафедра прикладної математики

# ВПЛИВ СОЦІАЛЬНИХ МЕРЕЖ НА КОРПОРАТИВНУ ІНФОРМАЦІЙНУ ТА ЕКОНОМІЧНУ БЕЗПЕКУ



**Здійснено огляд основних загроз інформаційної та економічної безпеки комерційних структур, що виникають у зв'язку з масовим поширенням сервісів соціальних мереж. Запропоновано також кілька засобів захисту від таких загроз.**

**Ключові слова: соціальна мережа, загроза, інформаційна безпека, економічна безпека, захист інформації.**

**The article reviews the main types of threats to information and economic security of business corporations, arising from widespread social networking services. The paper also proposes several means of protection against them.**

**Key words: social networks, threat, information security, economic security, data protection.**

## Вступ

Соціальні мережі – феномен XXI століття. Можна сміливо стверджувати, що серед користувачів ПК сьогодні не залишилось тих, хто не чув би про мережі на кшталт Facebook чи "ВКонтакте", а наявність облікового запису (account) хоча б в одній із відомих соціальних мереж стало невід'ємним атрибутом переважної більшості користувачів Інтернету. За даними, які були опубліковані в засобах масової інформації та мережевих ресурсах [1], у 2010 році в одній лише мережі Facebook користувачі провели загалом більше 700 млрд. хвилин.

Соціальні мережі почали своє існування як спосіб використання "мережі для зав'язування дружніх відносин та пошуку партнерів для романтичних стосунків". У наш час їх аудиторія зростає стрімкими темпами. Соціальні мережі проникли в усі сфери життя. Зокрема, як відзначають експерти, вони стали одним із основних комунікаційних каналів у розвитку ділових відносин. За даними першого щорічного дослідження "Індекс ризику соціальних мереж для підприємств малого і середнього бізнесу" [2], який проводився компанією Panda Security – продавцем програмних засобів захисту, 78 % опитаних підприємств у 2010 році використовували соціальні мережі для моніторингу діяльності конкурентів, покращення якості обслуговування, а також для просування своєї продукції, проведення маркетингових програм та збільшення доходу. Завдяки цьому типу соціальних медіа змінюються способи взаємодії організацій з клієнтами, формування брендів і спілкування з оточуючим світом. Більше того, компанії, які не братимуть до уваги чинник впливу соціальних мереж на клієнтів, за прогнозами аналітиків, втрачатимуть контакт з ринком і упускатимуть можливості для розвитку свого бізнесу.

Але ті ознаки, які роблять соціальні мережі таким привабливим середовищем спілкування, а саме: персоніфікація, простота, з якою можна ділитися інформацією, спілкування в режимі чат – водночас ховають в собі значні ризики для бізнесу. У сучасному "соціальному світі без кордонів" немає обмежень не тільки для комунікацій, а й для найвитонченіших злочинів.

**Мета роботи –** виявити і проаналізувати існуючі загрози, з якими неминуче доведеться стикнутися, використовуючи соціальні мережі у бізнесі, й на основі проведеного аналізу запропонувати можливі способи їх усунення.

**Загрози соціальних мереж**

Соціальні мережі є квінтесенцією сучасних Web-технологій. Вони містять і всі загрози, властиві Інтернету, які можна поділити на великі групи.

*Шкідливе програмне забезпечення (ПЗ).* За даними компанії Sophos [3], для 40 % власників ПК джерелом шкідливого ПЗ стали сайти підтримки соціальних мереж. А уже згадувані дослідження "Індекс ризику соціальних мереж для підприємств малого і середнього бізнесу" компанії Panda Security виявили, що 33 % із 315 опитаних у США компаній малого бізнесу відчули вплив щонайменше одного шкідливого програмного продукту із соціальних мереж. 35 % із цієї "інфікованої" групи відзначили, що вони потерпіли фінансові збитки у результаті такого порушення безпеки їх комп'ютерів. Також за підсумками досліджень [2], стає зрозуміло, що найчастішою причиною зараження шкідливим ПЗ (71,6 %) і порушення конфіденційності (73,2 %) є Facebook. Друге місце за кількістю зараження шкідливим ПЗ посідає YouTube (41,2 %), у той час, як Twitter став причиною значної кількості порушень конфіденційності (51 %). Серед компаній, які зазнали фінансових втрат через витік даних, на першому місці знову виявився Facebook (62 %), потім Twitter (38 %), YouTube (24 %) і LinkedIn (11 %).

Інструментами Web-атак кіберзлочинців є "троянські" програми, фальшиві антивіруси, соціальні хробаки, які використовують для власного розповсюдження списки "друзів".

Проблемою сайтів багатьох соціальних мереж, зокрема є те, що їх параметри, встановлені за замовчуванням, роблять користувачів уразливими. Ті, у кого недостатньо знань у сфері інформаційної безпеки, можуть і не підозрювати про необхідність зміни налаштувань з метою власного захисту. Наприклад, за замовчуванням сайти соціальних мереж можуть дозволяти використання HTML у коментарях, що дає змогу їх користувачам обмінюватися гіперпосиланнями, вставляти картинки тощо. Власне це і спрощує хакеру завдання впровадження шкідливого ПЗ, бо дає можливість вставити в такий спосіб посилання на розташований за межами сайту шкідливий код, який, наприклад, може відкрити зловмисникам доступ до внутрішньої мережі компанії.

Для захисту від описаних Web-атак необхідно використовувати такі традиційні засоби, як антивіруси, що вміють працювати у режимі реального часу, блокуючи завантаження шкідливих кодів.

*Крадіжка паролів і фішинг.* Як відомо, для ідентифікації соціальні мережі використовують паролі. Щоб їх отримати зловмисники використовують фішинг, підставні сайти, соціальну інженерію та інші методи. А знаючи пароль, можна від чужого імені, наприклад, розсилати рекламу – носія шкідливого ПЗ і робити інші недозволені речі.

Зловмисники розраховують на те, що більшість користувачів для усіх своїх облікових записів використовують один і той самий пароль доступу. Тоді в результаті зламу користувацького запису соцмережі значно підвищується імовірність проникнення до корпоративних ресурсів від імені одного із працівників, якщо у цього працівника є звичка використовувати одні й ті самі ім'я користувача та пароль у корпоративній та у зовнішній соціальній мережах. Також у кібершахрая з'являється реальний шанс отримати доступ до облікового запису інтернет-банкінгу користувача зламаного аккаунта соцмережі у разі збігу паролів інтернет-банкінгу та використовуваного у соціальній мережі.

Деякі компанії застосовують соціальні мережі для просування своєї продукції, тому крадіжка паролю адміністратора групи дасть змогу вкрасти і саму групу, а тим самим і ринок збуту.

Захистом від описаних небезпек є дотримання усіх стандартних правил стосовно паролів, зокрема, періодична заміна паролю; використання DLP-систем та інтегрованих у антивірусні програми репутаційних технологій.

*Витік інформації.* Розміри офісу, його наповнення майном, кількість працівників і активність їхніх телефонних переговорів, наявність клієнтів і робота з ними, корпоративний стиль – усе це є непрямою вказівкою на розміри і прибутковість компанії. І про все це можна довідатись з інформації, викладеної її працівниками на особистих сторінках у соціальних мережах.

Що ж стосується питання конфіденційності, то трапляється, що навіть адміністратори корпоративних аккаунтів публікують для загального користування занадто багато відомостей, які

згодом можуть використовуватися зловмисниками проти самої компанії. Наприклад, можуть публікуватися деякі дані про корпоративні фінанси, робочий процес.

Також соціальні мережі можуть використовуватися для підриву репутації компанії. Таку цілеспрямовану атаку можуть провести її працівники, незадоволені керівництвом, конкуренти, ображені клієнти. Підірвати не стільки інформаційну безпеку компанії, скільки економічну, може компрометуюча поведінка працівників у соцмережах: приголомшуючі публікації, грубі репліки.

Існує багато компаній, для яких проблема витоку інформації є вкрай актуальною: переважно це є компанії, що працюють на ринку надання послуг, особливо фінансових і юридичних. Для таких компаній втрата репутації є рівнозначною втраті грошей. У зв'язку з цим багато організацій сповідують ідеологію, згідно з якою її співробітники не можуть користуватися нелегітимним ПЗ або неліцензованими фільмами, музикою, оскільки це може кинути тінь на імідж компанії.

Боротися з розглянутим типом загроз потрібно організаційними методами.

*Зниження продуктивності праці.* За даними досліджень Panda Security [2], 77 % працівників малого та середнього бізнесу використовують соціальні мережі у робочий час. При цьому керівнику надзвичайно важко налагодити, не встановлюючи відповідних заборон, нормальний контроль за тим, чим підлеглий займається у соціальних мережах. Відсутність такого контролю може завдавати шкоду економіці компанії.

*Ріст трафіку,* особливо під час перегляду відеоджерел. Майже 40 % працівників зауважують, що спілкування в соціальних мережах створює значне навантаження на інтернет-канал і сповільнює роботу мережевих програм, необхідних для ведення бізнесу [1]. Для перегляду одного лише відео в режимі онлайн вимагається від мережі пропускної здатності від 500 Кбайт/с до 1,2 Мбайт/с, а що стосується відео високої роздільної здатності (HD), то навантаження на мережу може збільшитися до 4–7 Мбайт/с. У випадку, коли десятки і сотні користувачів одночасно дивляться відео, пропускна здатність мережі, необхідна для роботи мережевих програм, неминуче падає. Як вихід з ситуації пропонується обмежити доступ до відеотрафіку тих категорій працівників, для яких перегляд відео не допоможе у виконанні посадових обов'язків.

**Заходи захисту інформації**

Для того, щоб справитися із зростаючими загрозами у сфері інформаційної безпеки, пов'язаними зі швидким розповсюдженням соціальних мереж, корпоративні спеціалісти повинні, не втрачаючи часу, впроваджувати ефективні методи для підтримки конкурентоспроможності своїх компаній. На щастя, сьогодні постачальникам продуктів та послуг у галузі IT-безпеки, інтеграторам рішень і розробникам корпоративних політик безпеки є що протиставити новому спектру загроз.

*Організаційні заходи.* Керівництву компаній необхідно проводити адекватну роз'яснювальну і просвітницьку роботу з персоналом, зокрема організовувати тренінги, які даватимуть елементарні знання з інформаційної безпеки, оскільки, за статистикою, 70 % витоку інформації відбувається через необережність та необізнаність працівників. Також необхідно посилити дисципліну працівників і відчуття відповідальність за володіння комерційною інформацією. Реалізація цих заходів передбачає доволі великий обсяг робіт: створення і доведення до відома працівників локальних нормативних актів, регламентів або інструкцій, впровадження режиму комерційної таємниці.

Слід зауважити, що організаційні методи – це частина комплексу робіт, які не замінять технічні засоби, а лише доповнять їх, і тільки вдале поєднання організаційних та технічних заходів дасть необхідний ефект в області захисту інформації.

*Технічні засоби* – комплексні засоби моніторингу, аналізу і фільтрації вхідного і вихідного трафіків на рівні шлюзів. Аналіз у режимі реального часу дасть можливість переглядати окремі з'єднання і виявляти чинники ризику, забезпечуючи тим самим своєчасний захист діяльності працівників компанії у соціальних мережах, зокрема і в Інтернеті загалом.

*Вибірковий контроль використання соціальних мереж.* Для захисту організації від витоку даних і для впевненості її керівника у тому, що працівники не порушують прийняті обмеження на

розповсюдження інформації, йому необхідно залишити за собою право слідкувати за діями своїх підлеглих на сайтах соціальних мереж. Наприклад, можна заборонити підлеглим здійснювати завантаження на сайти соціальних мереж текстових файлів, фотографій і відеозаписів. Це дасть змогу знизити ризик витоку даних і збереже репутацію компанії.

*Робота з використанням кеш-пам'яті.* Для зниження впливу соціальних мереж на пропускну здатність інтернет-каналу слід здійснювати кешування на сервері сторінок найзатребуваніших сайтів. Отже, після початкового завантаження із мережі файли даних і відеофайли будуть зберігатися на локальному сервері, що дасть змогу зменшити трафік і знизити час реакції на запит користувача. При цьому можна буде отримувати доступ до сторінок соціальних мереж (точніше на локальний сервер, де вони зберігаються і оновлюються), не знижуючи пропускну здатність мережі підприємства.

**Висновок**

Не підлягає сумніву, соціальні мережі – потужний інструмент маркетингу, просування товару, нарощування клієнтської бази. Ми не пропонуємо відмовитися від соціальних мереж, оскільки з точки зору забезпечення бізнес-процесів багатьох сучасних компаній – це просто неможливо. Ми закликаємо мінімізувати загрози, пов'язані з необережною поведінкою користувачів соціальних мереж. Керівництво компаній має зрозуміти, що проекти Web 2.0 – це не просто дешеві джерела корисної маркетингової інформації, вони можуть нести багаточисленні загрози бізнесу. Лише системний підхід до управління підприємництвом і його безпекою, коли усі працівники, особливо у кризових, конфліктних і нестабільних ситуаціях, серйозно ставитимуться до проблеми забезпечення інформаційної, особистої безпеки і економічної безпеки організації загалом, дасть позитивні результати діяльності. А для цього менеджерам і фахівцям служби безпеки організації необхідно ретельно освоїти і ефективно застосовувати основні засоби управління організацією, персоналом і системою безпеки у підприємницькій діяльності.

*1. Найджел Хоторн. Социальные сети без риска. – [Електронний ресурс]. – Режим доступу:* http://www.s-director.ru/publ/view/58.html. *2. Арсентьев А. Социальные сети: киберпреступники ставят ловушки на СМБ. – [Електронний ресурс]. – Режим доступу:* http://www.cnews.ru/news/top/index.shtml?2011/03/02/430417. *3. Риск социальных сетей для малого бизнеса. – [Електронний ресурс]. – Режим доступу :*http://web-by.com/social_nets.