СЕКЦІЯ 6

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

Аровіна М. П., канд. наук з держ. упр., доцент
Донецький національний університет імені Василя Стуса, м. Вінниця

ЗАХИСТ ІНСТРУМЕНТІВ КОМУНІКАЦІЇ СОЦІАЛЬНИХ МЕРЕЖ

Соціальна мережа – Інтернет-співтовариство користувачів, об'єднаних за певною ознакою на одному веб-ресурсі [1]. У наш час у світі існує більше 200 великих соціальних мереж, 15 мають більше 100 мільйонів активних користувачів; Facebook, Twitter, Instagram, LinkedIN, Google+ тощо [2].

Метою функціонування будь-якої соціальної мережі є процес Інтернет-комунікації. Це сукупність методів спілкування, коли інформація передається на основі стандартних протоколів Інтернет. Соціальні мережі можна класифікувати таким чином (табл. 1).

Таблиця 1

Класифікація соціальних мереж [2]

Клас соціальних мереж	Ознака класифікації	Представники
Загально форматні соціальні мережі	Неформальне спілкування користувачів	Facebook, Qzone, MySpace, Google+, YouTube
Професійні соціальні мережі	Професійне спілкування користувачів	Social network for scientists, LinkedIN, E-xecutive
Соціальні мережі за інтересами	Спілкування користувачів, об'єднаних спільними інтересами	Facebook, LinkedIN, Studnet, Renren Network

Залежно від інтересів користувачів та кола учасників, комунікації у соціальних мережах можуть бути міжособистісними, міжгруповими, міжсоціумними. При цьому реалізуються різноманітні форми передачі інформації: аудіо-, відео-, графічні файли, текстові документи, миттєві повідомлення тощо. Відповідно, інструменти комунікації теж різняться. Умовно їх можна поділити на дві групи: активні (що мають зворотний зв'язок) і пасивні (табл. 2).

Таблиця 2

Класифікація інструментів комунікацій в соціальних мережах

Активні інструменти	Приклади	Пасивні інструменти	Приклади
Електронна пошта e-mail	Facebook (username@facebook.com Google+ username@gmail.com	Розподілена система управління базами даних	Apache Cassandra
Месенджери Short Message Service (SMS), Internet Relation Chat (IRC)	Facebook Chat, Renrenzhuomian Google Talk	Служби пошуку даних і програм	Archie Whois Gopher WAIS Google search

Сервіс відео дзвінків	Facebook Messenger Служба відправки повідомлень	Пости в соціальних мережах або твіти	Facebook Twitter Instagram
Телеконференції	Facebook (UseNet) Google+ (Google Hangouts)	News - групи новин	Facebook Twitter

На сьогодні, незважаючи на значну поширеність соціальних мереж, проблема безпеки залишається однією з найбільш актуальних. Крім цього, її загостренню сприяє користування соціальними мережами через мобільні пристрої, які є більш вразливими для атак хакерів, ніж персональні комп'ютери. За даними «Google Україна», серед молодих людей у віці до 35 років 72 % українців використовують смартфони. Загалом з 2013 року кількість користувачів смартфонів в Україні зросла на 150 % – у два з половиною рази. Соціальні мережі є найбільш популярною сферою використання цих пристроїв – 42 % всіх дій [3].

До основних загроз щодо інструментів комунікацій віднесемо такі:

- фішинг (англ. *phishing,* від *fishing* – риболовля, видобування) – вид комп'ютерного шахрайства, основна мета якого – обманним шляхом змусити жертву надати шахраєві потрібну йому інформацію. Це комп'ютерний злочин, який переслідується законом [4].
- фармінг (англ. *pharming*) – це процедура таємного перенаправлення жертви на помилкову IP-адресу. Для цього може використовуватися навігаційна структура (файл hosts, система доменних імен (DNS)).
- атаки, основані на прослуховуванні мережевого з'єднання, наприклад, сніфферські (перехоплення трафіка) або атаки типу man-in-the-middle (втручання в канал зв'язку).

Слід зазначити, що способи захисту інструментів комунікацій в соціальних мережах можна поділити на загальні та специфічні. До загальних належать:

- установка на комп'ютері або мобільному пристрої антивірусних програм (наприклад, Panda Antivirus або AVG AntiVirus, які діють на різних платформах, таких як Mac, Android та Windows);
- використання системи запобігання мережевим атакам (Intrusion Prevention System) дозволяє виявляти ознаки атак ще на ранніх стадіях дій зловмисників та істотно знизити втрати компанії від дій хакерів і хактивістів (наприклад, Check Point IPS Software Blade, Cisco FirePower, HP TippingPoint, McAfee Security Gateway);
- регулярне очищення даних про профіль користувача соціальної мережі, які залишаються браузером у вигляді файлів або записів;
- застосування протоколу https при вході і перебування в мережі, що дозволяє всі дані, які передаються між користувачем і серверами, у тому числі логін і пароль, «упаковувати» в криптографічний протокол SSL або TLS. Таким чином забезпечується захист даних від атак, основаних на прослуховуванні мережевого з'єднання;
- уникнення комунікацій з невідомими користувачами і додатками соціальної мережі (фішингу та фармінгу) [5].

Спеціальні способи захисту: доступ до соціальних мережі через спеціалізовані криптографічні браузери (наприклад, Tor, Onion Browser). Такі технології забезпечують захист від механізмів аналізу трафіку, які загрожують приватності, конфіденційності ділових контактів і таємниці зв'язку в цілому [6].

Список використаних джерел

1. Соціальна мережа [Електронний ресурс]. – Режим доступу: igroup.com.ua/seo-articles/sotsialna-merezha/

2. Калужский М. Л. Сетевые интернет-коммуникации как инструмент маркетинга [Електронний ресурс] / М. Л. Калужский, В. В. Карпов. – Режим доступу: http://www.aup.ru/articles/marketing/52.htm

3. Особливості національного інтернету. [Електронний ресурс]. – Режим доступу: http://zaxid.net/news/showNews.do?osoblivosti_natsionalnogo_internetu&objectId=1403421

4. Фишинг. Советы по безопасности. Официальный сайт Dr.Web антивирус [Електронний ресурс]. – Режим доступу: http://antifraud.drweb.ua/phishing/?lng=ru

5. Запобігання мережевим атакам [Електронний ресурс]. – Режим доступу: http://www.bms-consulting.com/uk/service/netsecurity/

6. What is Tor Browser? [Електронний ресурс]. – Режим доступу: https://www.torproject.org/projects/torbrowser.html.en

Лаврентьєва Л. В.
Маріупольський державний університет, м. Маріуполь

ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ РІВНЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Сьогодні розвиток сучасних підприємств доволі тісно пов'язаний з рівнем його економічної безпеки, бо тільки за таких умов існує можливість для ефективного стратегічного планування операційної діяльності, управління й якісного контролю за діяльністю як внутрішньо-, так і зовнішньогосподарською, а також побудови вигідних економічних відносин з іншими суб'єктами господарювання. Тенденція до зниження рівня економічної безпеки вітчизняних підприємств здебільшого обумовлена інерційністю їхньої структури виробництва, значним фізичним зносом обладнання, низькою інноваційною активністю. Тому дедалі більшої актуальності набуває питання необхідності практичного дослідження рівня економічної безпеки.

Рівень економічної безпеки підприємства є найважливішим показником економічної безпеки підприємства, під яким слід розуміти оцінку стану використання внутрішньоорганізаційних ресурсів за критеріями рівня економічної безпеки підприємства.

Рівень економічної безпеки підприємства не можна оцінити певним статичним показником, оскільки він містить, як мінімум, три компоненти: існуючий