Все це вимагає вашого часу, зусиль, терпіння, знань. Просувайте і продавайте не вашу компанію, а «емоцію», яку несе товар або послуга. Наприклад, турів до Туреччини за доступними цінами повно, а от повне відключення від поточних турбот і занурення в двотижневий релакс – явище рідкісне.

Перелік використаних джерел

1. https://aptxt.com/category/dostupno-o-kopirajtinge

Ладига Поліна
студент, кафедра міжнародної торгівлі та права, 4 група, 2 курс
Київський національний торговельно-економічний університет,
м. Київ, Україна
Polina Ladyga,
Student of the Department of International Trade and Law,4 group, 2nd year,of the
Kyiv National University of Trade and Economics,
Kyiv, Ukraine
Науковий керівник: **Жук Олена Сергіївна**
к.е.н, асистент кафедри економіки та фінансів підприємства,
Київський Національний Торговельно-Економічний Університет
Scientific supervisor: **Olena Zhuk**
Candidate of Economic Sciences,
Assistant of the Department of Economics and Business Finance of the
Kyiv National University of Trade and Economics,

ЕКОНОМІЧНА БЕЗПЕКА БІЗНЕСУ ТА СОЦІАЛЬНІ МЕРЕЖІ, ЯК ІНСТРУМЕНТ РОЗВИТКУ БІЗНЕСУ
ECONOMIC SECURITY OF BUSINESS AND SOCIAL NETWORK AS THE TOOL FOR BUSINESS DEVELOPMENT

Соціальні мережі виступають, як виключно феномен XXI століття. На наш погляд, можна не просто сміливо стверджувати, що зараз вже не залишилось жодного користувача портативного комп'ютера, які хоча б раз не використовували такі соціальні мережі як «Facebook» чи «Instagram».

За останніми даними, які є в широкому доступі, та опубліковані засобами масової інформації, у 2017 р. кількість користувачів «Facebook» досягла близько двох мільярдів [1].

Спочатку соціальні мережі існували як засіб для власного користування між будь-ким з користувачів Інтернету, які мають власний профіль чи сторінку. Але, з часом вони стали більш комерційними. Зараз соціальні мережі виступають, як головний засіб для рекламного інтегрування та приносять великі кошти власникам популярних сторінок. Як приклад, можна відзначити таке явище як «Influencer marketing». Це така форма маркетингу, в якій акцент робиться на впливових людей, а не цільовий ринок в цілому. Вона визначає осіб, які впливають на потенційних покупців, і орієнтує маркетингову діяльність навколо цих впливових осіб [1].

Соціальні мережі проникли у всі сфери життя. Зокрема, вони стали одним із основних комунікаційних каналів у розвитку ділових відносин.

Наприклад, якщо взяти до уваги офіційну статистику, лише за 2016 рік за дослідженням компанії Panda Security («Індекс ризику соціальних мереж для підприємств малого і середнього бізнесу») близько 90% учасників опитування серед власників підприємства та їх співробітників використовували соціальні мережі для моніторингу діяльності конкурентів, покращення якості обслуговування, а також для просунення своєї продукції, проведення маркетингових програм та збільшення доходу [2].

Основні фактори, які роблять соціальні мережі привабливими для ведення бізнесу - це саме можливість персоніфікації даних, простота у користуванні, спілкування у вигляді чату в реальному часі. Та, водночас, всі ці позитивні фактори створюють величезний ризик для бізнесу. І

головною метою є саме виявлення та ідентифікація саме загроз соціальної мережі в сфері економічної безпеки, а також можливість створення більш «захищених» умов для користувачів.

Соціальні мережі, як й всі WEB-технології, мають подібні загрози. Перш за все потрібно відзначити шкідливе програмне забезпечення (далі ПЗ). За останніми даними, які надає компанія Sophos для 40% власників портативного комп'ютера джерелом шкідливого ПЗ стали сайти, як би це не було іронічно саме підтримки соціальних мереж. А уже згадувані дослідження «Індекс ризику соціальних мереж для підприємств малого і середнього бізнесу» компанії PandaSecurity виявили, що близько 45% із 315 опитаних в США та Канаді компаній малого та середнього бізнесу відчули влив щонайменше одного шкідливого програмного продукту із соціальних мереж [3].

За підсумками дослідження найчастішою причиною зараження ПЗ (71,6%) і порушення конфіденційності (73,2%) є «Facebook». Друге місце за кількістю зараження шкідливим ПЗ займає YouTube (41,2%), у той час як Twitter став причиною значної кількості порушень конфіденційності (51%) [2].

Головними інструментами Web-атак є троянські програми та неліцензійні антивірусні програми.

Серед інших загроз, які можуть впливати на користувачів, які використовують соціальні мережі, як для ведення бізнесу так і для власного користування є:

1. Фішинг. Всім відомо, що соціальні мережі використовують паролі. Для того, щоб їх отримати зловмисники використовують так звані «підставні сайти». Отримуючи сторонні паролі можуть використовувати аккаунти користувачів для розповсюдження реклами та спаму.

2. Витік інформації. Більшість з нас намагається показати своє життя з найкращої сторони – численні фотографії авіаційних квитків та приватні фотографії ставлять під загрозу не лише безпеку бізнесу, а й простих користувачів, вже не кажучи про численні шахрайства в соц. мережах (вже не раз у ЗМІ з'являлася інформація про те, як необачливі користувачі виставляють фотографії із штрих-кодом квитків) [4].

3. Ріст трафіку, який може бути спричинений DOS та DDOS атаками (відмова в обслуговувані користувачів, із-за перенавантаження трафіку ботами, тобто неіснуючими користувачами, яскравим прикладом цього є «Тролі з Ольгіа»).

Важливим фактором є саме те, що соціальні мережі стають більш адаптованими для ведення бізнесу. В «Instagram» з'являються спеціальні функції, які надають змогу просувати власні профілі та товари. Ні для кого не секрет, що на рекламному інтегруванні блогери з мільйонною аудиторію отримують величезні доходи. Не підлягає сумніву, соціальні мережі – потужний інструмент маркетингу, просування товару, нарощування клієнтської бази, тому дуже важливим є мінімізація загрози, пов'язана з необережною поведінкою користувачів соціальних мереж.

Перелік використаних джерел

1. Число пользователей Facebook достигло 2 млрд/ человек [Електронний ресурс] / Режим доступу: https://www.rbc.ru/technology_and_media/27/06/2017/5952994e9a7947329cd8627b .

2. Арсентьев А. Социальные сети: киберпреступники ставят ловушки на СМБ [Електронний ресурс] / А. Арсентьев. – 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.

4. Почему не стоит выкладывать фотографии билетов и ключей в социальные сети [Електронний ресурс]. – Режим доступу: https://tjournal.ru/59171-pochemu-ne-stoit-vykladyvat-fotografii-biletov-i-klyuchey-v-socialnye-seti.