ПЕДАГОГІКА

УДК 378.016:(005.334:005.332.4)

УПРАВЛІННЯ РИЗИКАМИ ЯК ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ ЗАКЛАДУ ВИЩОЇ ОСВІТИ

Л. А. Безносюк, І. М. Зарішняк

Анотація. У даному дослідженні розглянуто основні загрози, що впливають на підвищення конкурентоспроможності закладу вищої освіти. Серед них ті, що виникають під час розповсюдження рекламних повідомлень у соціальних мережах, зокрема підрив репутації закладу вищої освіти, зниження продуктивності праці, витік інформації, крадіжки паролів і шкідливе програмне забезпечення. Запропоновано шляхи управління захистом інформації на власних сторінках та захисту ділової репутації при розповсюдженні рекламних повідомлень на офіційних сторінках закладу вищої освіти.

Ключові слова: конкурентоспроможність; ризики; соціальні мережі; освітні послуги; система управління.

У процесі еволюції суспільства можна спостерігати активне зростання конкуренції майже у всіх ланках соціально-економічної системи. Не винятком є й сфера освіти. Для забезпечення та збереження конкурентних позицій на ринку освітніх послуг навчальні заклади змушені вдаватись до все нових і нових підходів та маркетингових рішень.

Для досягнення максимальної ефективності освітньої діяльності важливе значення має процес прийняття управлінських рішень пов’язаних з просуванням та підтримкою конкурентних переваг закладу освіти.

На сучасному етапі використання соціальних мереж є не лише засобом комунікації, а й можливістю для просування нових товарів та послуг, створення конкурентоспроможного бренду за допомогою реклами на ринку освітніх послуг. Протягом усього часу, що користувач знаходиться в мережі, він перебуває в зоні інформаційного впливу, що чиниться соціальними мережами, тож не використовувати таку чудову можливість для просування брендів, товарів або послуг було б для підприємств та рекламодавців вкрай необачно [1].

Загалом, діяльність будь-якого підприємства завжди пов’язана з ризиком. Але для втримання та збереження своїх конкурентних позицій на ринку освітніх послуг закладу вищої освіти необхідно регулярно аналізувати та проводити оцінку ризиків, аби мати змогу вчасно виявити загрози та попередити їх.

Використання соціальних мереж, та й взагалі реклами в інтернеті, в процесі підвищення конкурентоспроможності закладу вищої освіти несе певні загрози та ризики, які можна поділити на декілька груп (рис. 1).

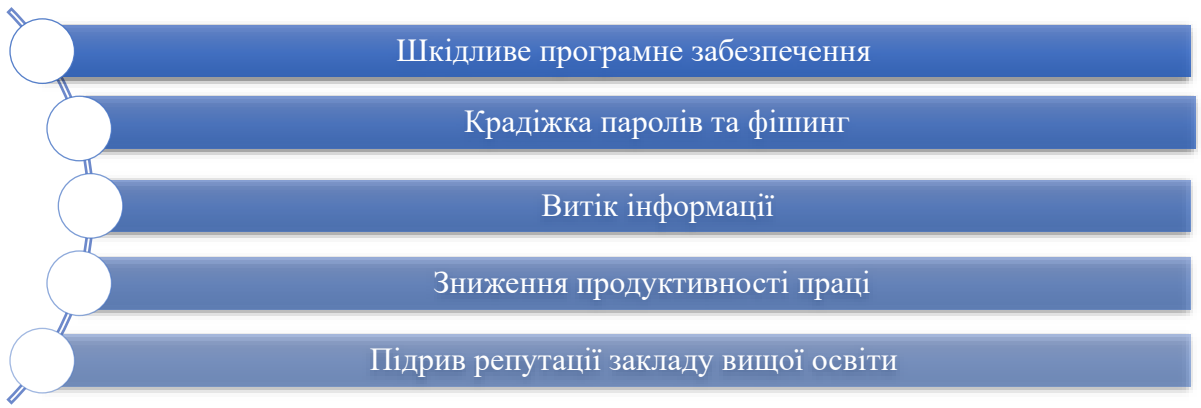

Рис. 1. Загрози, що виникають при роботі в мережі

За даними компанії Sophos, для 40 % власників ПК джерелом шкідливого ПЗ стали сайти підтримки соціальних мереж. А 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 що найменше одного шкідливого програмного продукту із соціальних мереж [2].

Проблемою сайтів багатьох соціальних мереж зокрема є те, що їх параметри встановлені за замовчуванням і тому роблять користувачів уразливими. Ті, у кого недостатньо знань у сфері інформаційної безпеки, можуть і не підозрювати про необхідність зміни налаштувань з метою власного захисту. Для захисту від описаних Web-атак при використанні мережі для просування закладу вищої освіти необхідно використовувати такі традиційні засоби, як анти віруси, що вміють працювати у режимі реального часу, блокуючи завантаження шкідливих кодів [3].

Ще однією насущною проблемою є крадіжка паролів і фішинг (вид шахрайства, метою якого є вилучення особистих даних у користувачів мережі, шляхом обману, шахрайських дій). При реєстрації та створенні сторінки у будь-якій соціальній мережі для ідентифікації необхідно обов'язково використовувати паролі. Щоб їх отримати, зловмисники використовують фішинг, підставні сайти, соціальну інженерію, фальшиві розсилки та інші методи. А знаючи пароль, можна від чужого імені, наприклад, розсилати рекламу – носія шкідливого ПЗ і робити інші недозволені речі.

Для закладу вищої освіти, що застосовує соціальну мережу для просування своїх товарів та послуг, крадіжка паролів є великим ризиком, що, в свою чергу, може призвести до фатальних наслідків та втрати власних конкурентних позицій. Захистом від описаних небезпек є дотримання усіх стандартних правил стосовно паролів (використання різного регістру, застосування літер та цифр, використання спеціальних символів тощо), зокрема, періодична заміна паролю; використання інтегрованих антивірусних програм тощо [3].

Також соціальні мережі можуть використовуватися для підриву репутації закладу вищої освіти. Таку цілеспрямовану атаку можуть провести власні працівники вишу, незадоволені керівництвом, конкуренти тощо. Підірвати не стільки інформаційну безпеку вишу, скільки економічну, може компрометуюча поведінка працівників у соцмережах: приголомшуючі публікації, грубі репліки, особисті переписки тощо.

Але, щоб не втрапити у халепу, керівництву закладу вищої освіти, необхідно вживати заходи щодо захисту інформації на власних сторінках та захисту ділової репутації в соціальних мережах та й взагалі в мережі (рис. 2).

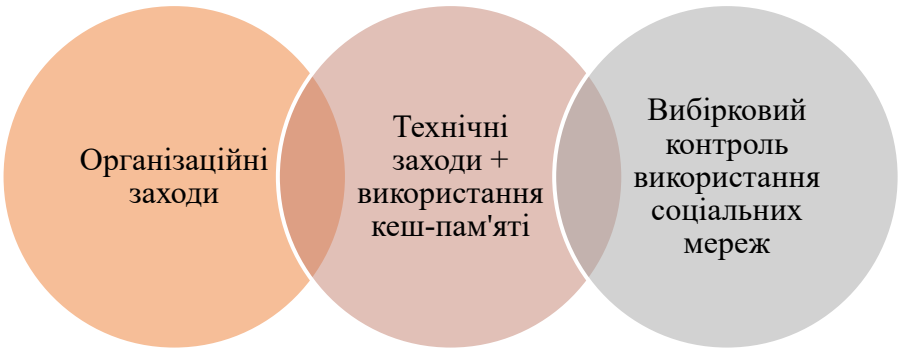

Рис. 2. Управління захистом інформації при роботі в соціальних мережах

До організаційних заходів захисту інформації при роботі у соціальних мережах можна віднести різноманітні тренінги, семінари, що проводяться з метою підвищення знань з інформаційної безпеки для студентів, співробітників та професорсько-викладацького складу. У процесі навчання необхідно наочно демонструвати, відтворюючи на прикладі загрозливі ситуації та шляхи протидії, уникнення та попередження негативного досвіду при роботі в мережі.

Технічні засоби – комплексні засоби моніторингу, аналізу і фільтрації вхідного і вихідного трафіку на рівні шлюзів. Використання сучасних технологій та аналіз у режимі реального часу дасть можливість переглядати окремі з'єднання і виявляти чинники ризику, забезпечуючи тим самим своєчасний захист діяльності працівників вишу у соціальних мережах, зокрема і в мережі Інтернет загалом [3].

Також для більш ефективнішої роботи та зниження впливу соціальних мереж на пропускну спроможність інтернет-каналу необхідно здійснювати кешування на сервері, тобто тимчасово зберігати відносно статичні дані в кеші і використовуючи ці дані з кешу, коли для цього буде необхідність, що дозволить економити час для генерації інших даних. Це дасть змогу швидше реагувати на повідомлення потенційних клієнтів, що в свою чергу полегшить комунікацію з цільовою аудиторією, підвищить зацікавленість до розповсюджуваної інформації та покращить позиції вишу на конкурентному ринку.

Але тільки вміле поєднання організаційних заходів та технічних засобів може призвести до успішної та безпечної роботи. Адже набуті знання і навички роботи в мережі та їх практичне застосування за допомогою сучасних інформаційних технологій призведе до убезпечення власних конкурентних переваг від зловмисних намірів та сприятиме створенню якісного контенту, що, в свою чергу, призведе до зростання зацікавленості до пропонованих пропозицій та підвищення конкурентоспроможності вишу на ринку освітніх послуг.

Щодо вибіркового контролю за використанням соціальних мереж, то керівник, як адміністратор сторінки, у тій чи іншій соціальній мережі має доступ до перегляду повідомлень, що надійшли або були надіслані з корпоративної сторінки. Тому він може з легкістю впевнитись в тому, що працівники не порушують умови конфіденційності корпоративної інформації та не підривають імідж закладу вищої освіти [3, 4].

Також, ще одним дискусійним питанням є те, що деякі роботодавці забороняють своїм підлеглим під час робочого часу користуватися соціальним мережами. З одного боку, дане рішення є правильним, адже працівники будуть більш сумлінніше виконувати свої обов'язки та не відволікатись на розваги та обмін особистими повідомленнями з друзями, родичами у соціальних мережах, що в свою чергу знижує продуктивність праці та виникають ризики витоку корпоративної інформації.

Але з іншого боку, завдяки соціальним мережам співробітники будь-якого вишу можуть проводити активні дії щодо розповсюдження реклами про діяльність закладу вищої освіти на власних сторінках. Здійснювати це можна шляхом репосту інформаційних публікацій із корпоративних сторінок вишу на свої власні, що в свою чергу призведе до охоплення більшого кола користувачів мережі, збільшить число зацікавлених та сприятиме підвищенню конкурентоспроможності на ринку освітніх послуг.

Висновки. Отже, соціальні мережі – це потужний інструмент для просування товарів та послуг закладів вищої освіти. Завдяки їм ми можемо не тільки розширити коло клієнтів, надаючи їм цікаві пропозиції в мережі, а й підвищити власну конкурентоспроможність на ринку освітніх послуг. Але без вживання необхідних заходів щодо забезпечення безпеки корпоративної інформації, власного іміджу та позицій на ринку, ця справа може зазнати краху. Управління захистом інформації при роботі в соціальних мережах передбачає застосування організаційних, технічних та контролюючих засобів запобігання та протидії виникненню ризиків та загроз при роботі в мережі, а саме проведення інструктажів для працівників вишу, щодо інформаційної безпеки при роботі в мережі, використання новітніх інформаційних технологій для захисту інформації розповсюдженої за допомогою каналів комунікації, впровадження контролюючих дій, стосовно діяльності в соціальних мережах та забезпечення ефективної та швидкої роботи шляхом кешування аби швидше реагувати на потенційних запити клієнтів. Тому працівникам, що відповідають за наповнення сторінок в соціальних мережах і фахівцям служби безпеки вишу, необхідно ретельно освоїти і ефективно застосовувати основні засоби та заходи безпеки управління діяльністю при роботі в мережі.

Аннотация. В данном исследовании рассмотрены основные угрозы, влияющие на повышение конкурентоспособности учреждения высшего образования. Среди них те, что возникают во время распространения рекламных сообщений в социальных сетях, в частности подрыв репутации учреждения высшего образования, снижение производительности труда, утечка информации, кражи паролей и вредоносное программное обеспечение. Предложены пути управления защитой информации на собственных страницах и защиты деловой репутации при распространении рекламных сообщений на официальных страницах учреждения высшего образования.
Ключевые слова. Конкурентоспособность; риски; социальные сети; образовательные услуги; система управления.

Abstract. This study examines the main threats to improving the competitiveness of higher education. These include social media advertising, including undermining the reputation of higher education institutions, declining productivity, information leakage, password theft, and malware. Ways to manage the protection of information on its own pages and the protection of business reputation in the distribution of advertising messages on the official pages of higher education institutions.
Keywords. Competitiveness; risks; social networks; educational services; management system.

СПИСОК ЛІТЕРАТУРИ

1. Бєлєнький П. Ю. Дослідження проблем конкурентоспроможності. *Вісник НАН України*. 2007. № 5. С. 9–18.

2. Риск социальных сетей для малого бизнеса. URL: http://web-by.com/social_nets/.

3. Кухарська Н. П., Кухарський В. М. Вплив соціальних мереж на корпоративну, інформаційну та економічну безпеку. *Вісник Національного університету «Львівська політехніка»*. 2012. № 741 : Автоматика, вимірювання та керування. С. 214–217.

4. Радзінькова М. Ю. Соціальні мережі як засіб системи маркетингових комунікацій сучасних підприємств. *Міжнародний науковий журнал «Інтернаука» Серія: «Економічні науки»*. 2018. № 7 (15). С. 69–74.

УДК 316.28

АНАЛІЗ ОСОБЛИВОСТЕЙ МОДЕЛЕЙ КОМУНІКАЦІЙНИХ ПРОЦЕСІВ

Т. С. Калініченко, К. С. Безгін

Анотація. У даному дослідженні надано інформацію про особливості моделей комунікаційних процесів. Наведено визначення ключових характеристик і змісту дефініції «комунікацій» різними авторами. У роботі представлено аналіз різновидів лінійних та нелінійних моделей комунікаційного процесу. У ході дослідження виявлено основні переваги та недоліки цих моделей. Запропоновано для дослідження комунікацій та побудови моделей комунікаційного процесу використовувати синтез методів штучного інтелекту та досліджень поведінки суб'єктів установи.
Ключові слова: комунікація, комунікаційні процеси, лінійні моделі комунікаційних процесів, нелінійні моделі комунікаційних процесів.

Вступ. В сучасних умовах невизначеності для сталого розвитку такої некомерційної установи як Донецький національний університет імені Василя Стуса необхідний пошук нових джерел підвищення ефективності діяльності. З огляду на вищезазначений статус некомерційної організації особливу роль може зіграти поліпшення таких нематеріальних факторів, як комунікаційні процеси установи.

Аналіз останніх досліджень і публікацій. Тематиці комунікаційних процесів на підприємствах присвячено праці багатьох вітчизняних науковців, таких як А. В. Боднар [1], В. А. Панченко [2], З. І. Єрмакова [3], Ю. В. Міронова, О. О. Кагляк, О. В. Пітик [4]. Проте слід зазначити, що кількість публікацій, присвячених тематиці комунікацій значно більша, ніж комунікаційних процесів, що надає актуальності даному дослідженню.

Метою статті є дослідження теоретичних основ моделювання комунікаційних процесів.