© Peleshchyshyn A., Trach O. Determination of elements of socio-oriented risks by organization of the life cycle of the virtual community // Ukrainian Scientific Journal of Information Security, 2017, vol. 23, issue 2, p. 130-135.

DOI: 10.18372/2225-5036.23.11802

ВИЗНАЧЕННЯ ЕЛЕМЕНТІВ СОЦІАЛЬНО-ОРІЄНТОВАНИХ РИЗИКІВ ПРИ ОРГАНІЗАЦІЇ ЖИТТЄВОГО ЦИКЛУ ВІРТУАЛЬНОЇ СПІЛЬНОТИ

Андрій Пелещишин, Ольга Трач

Національний університет «Львівська політехніка», Україна

ПЕЛЕЩИШИН Андрій Миколайович, д.т.н.

Рік та місце народження: 1973 рік, м. Львів, Україна.
Освіта: Львівській Державний університет ім. І.Франка, 1995 рік.
Посада: завідувач кафедри соціальних комунікацій та інформаційної діяльності Національного університету «Львівська політехніка» з 2011 року.
Наукові інтереси: истемотворчі процеси WWW, методи побудови інформаційного суспільства, позиціонування сайтів у WWW, соціальні мережі у WWW та інформаційні технології соціальних комунікацій.
Публікації: більше 200 наукових публікацій, серед яких монографії, підручники, навчальні посібники, наукові статті, матеріали та тези доповідей на конференціях.
E-mail: apele@ridne.net

ТРАЧ Ольга Романівна

Рік та місце народження: 1992 рік, м. Львів, Україна.
Освіта: Національний університет «Львівська політехніка», 2013 рік.
Посада: асистент кафедри соціальних комунікацій та інформаційної діяльності з 2015 р.
Наукові інтереси: соціальні комунікації у WWW, життєвий цикл віртуальних спільнот.
Публікації: більше 20 наукових публікацій.
E-mail: olya@trach.com.ua

Анотація. *У статті запропоновано соціально-орієнтовані ризики при організації життєвого циклу віртуальної спільноти, а саме: ризик появи негативно налаштованої аудиторії, ризик зниження якості інформаційного наповнення, ризик антизаконних матеріалів, ризик втрати контролю над спільнотою. Досліджуваним елементом соціально-орієнтованих ризиків є текстове інформаційне наповнення, що включає коментарі та пости у віртуальній спільноті. Запропоновані заходи з протидії соціально-орієнтованим ризикам, а саме: уникнення учасників провокаторів, усунення флеймерів, запобігання кібербулінгу, покращення якості інформаційного наповнення, покращення достовірності інформаційного наповнення, покращення рекламних оголошень, правова верифікація, уникнення плагіату, запобігання фітингу, формування лідера спільноти, керування лідером спільноти. Представлене визначення показника входження спільноти в зону соціально-орієнтованого ризику. Розроблено алгоритм визначення рівня інтенсивності заходів протидії соціально-орієнтованим ризикам. Здійснено класифікацію рівня ризиків на високий, середній та низький рівні.*

Ключові слова: *віртуальна спільнота, ризик, життєвий цикл, учасники, інформаційне наповнення.*

Вступ

Сьогодні віртуальні спільноти стали надзвичайно популярним явищем в бізнесі, в політиці, для задоволення власних потреб. В результаті чого віртуальні спільноти стали окремим видом професійної діяльності, зокрема окремим видом проекту. Одним з ключових питань в управлінні проектами є ризики при управлінні проектами. Дослідження показали, що найтиповішими ризиками в управлінні проектами є: ризик помилки проектування; ризик втрати робочої сили (виконавців етапів та напрямів); часові ризики; помилки адміністраторів та модераторів при управління спільнотою та ін. Число ризиків, які виникають при створенні віртуальної спільноти є значним. Проаналізувавши типові ризики управління проектами виділено соціально-орієнтовані ризики організації життєвого циклу віртуальної спільноти.

Аналіз існуючих досліджень

Сьогодні відслідковується значне збільшення віртуальних спільнот, розвиток уже існуючих, їхня популярність в багатьох сферах діяльності. Тому

актуальним питанням є дослідження віртуальної спільноти як окремого виду проекту, з своїми особливостями, характеристиками та функціями. Проте, дослідження ризиків при створенні та управлінні віртуальної спільноти є неповними. В проектному менеджменті одним з актуальних питань є управління проектними ризиками. Науковці значну увагу приділяють ризикам в проектному менеджменті, дослідження проводяться в таких напрямах як: методи та інструментарії аналізу ризиків в проектах [1-3], методології управління ризиками [4-5], заходи протидії ризикам [6-7].

Таким чином, *метою* даної роботи є визначення соціально-орієнтованих ризиків при організації життєвого циклу віртуальних спільнот, визначення заходів протидії ризикам та розроблення алгоритму визначення рівня інтенсивності заходів протидії соціально-орієнтованим ризикам при організації життєвого циклу віртуальних спільнот.

Основна частина дослідження

В ході виконання будь-якого етапу організації життєвого циклу віртуальної спільноти можуть з'являтись ситуації у яких окремі показники виходитимуть за межі передбачуваних значень, погіршуючи загальний стан виконання проекту. Такі ситуації фактично є ризиками, що виникають під час реалізації проекту. Число ризиків, які виникають є значним. Одними з притаманних віртуальній спільноті є соціально-орієнтовані ризики.

Соціально-орієнтовані ризики – це виникнення ситуації у яких окремі параметри показників виходитимуть за межі передбачуваних значень, погіршуючи загальний стан виконання проекту.

В процесі організації життєвого циклу віртуальної спільноти виділимо наступні соціально-орієнтовані ризики [8]:

– поява негативно налаштованої аудиторії;

– зниження якості інформаційного наповнення;

– антизаконні матеріали та діяльність спільноти;

– втрата контролю над спільнотою.

Система соціально-орієнтованих ризиків організації життєвого циклу віртуальної спільноти описується кортежем (1):

$$SOR(Com_i) = \left\langle \begin{matrix} NegativeAud^{(User)}(Com_i), InfContent^{(Inf)}(Com_i), \\ Antilegal^{(User,Inf)}(Com_i), Control^{(User)}(Com_i) \end{matrix} \right\rangle, \quad (1)$$

де $NegativeAud^{(User)}$ - ризик появи негативно налаштованої аудиторії; $InfContent^{(Inf)}$ - ризик зниження якості інформаційного наповнення; $Antilegal^{(User,Inf)}$ - ризик антизаконних матеріалів та діяльності спільноти; $Control^{(User)}$ - ризик втрати контролю над спільнотою.

В процесі виконання проектних робіт по формуванню віртуальної спільноти необхідно передбачити захист появи ризику, який передбачає заходи з протидії соціально-орієнтованим ризикам.

Ризик появи негативно налаштованої аудиторії. Соціально орієнтований ризик поява негативно налаштованої аудиторії полягає в тому, що у віртуальній спільноті з'являється підмножина користувачів, які негативно налаштовані щодо діяльності спільноти чи інших учасників спільноти. До заходів захисту від ризику появи негативно налаштованої аудиторії належать: уникнення учасників провокаторів; усунення флеймерів; запобігання кібербулінгу.

Уникнення учасників-провокаторів. Заходи протидії полягають у виявлені учасників, які створюють провокативну ситуацію, негативну обстановку щодо інших учасників чи діяльності віртуальної спільноти.

Провокатор – це учасник віртуальної спільноти, який своїми діями штучно створює негативну обстановку у віртуальній спільноті. Наприклад, учасник спільноти почав написати провокативні пости та коментарі проти діяльності спільноти, дані дії несуть за собою негативні наслідки.

До провокаторів можна віднести:

– троль – учасник віртуальної спільноти, який вступає у віртуальну спільноту з метою вчинення провокативних дії відносно інших учасників чи діяльності спільноти. Учасник спільноти здійснює роль троля методом ручного керування та з допомогою спеціалізованих програмних засобів – роботів, або з використанням цих двох методів [9];

– користувач з нестійким психо-емоційним станом – учасник віртуальної спільноти, який в силу своїх психічних розладів чинять дії спрямовані на провокування інших учасників.

Учасників-провокаторів (зокрема тролів) у віртуальній спільноті можна виділити за:

1. Рейтингом:

– учасник-троль з високим рейтингом. Учасник віртуальної спільноти має високий рейтинг, проте його дописи, аватар та нік-нейм свідчать про те, що він троль;

– учасник-троль з низьким рейтингом. Ще одна ознака учасника-троля – це мінусовий рейтинг, знижений за порушення.

2. Стилем спілкування: учасник-провокатор відрізняється від решти учасників віртуальної спільноти стилістикою спілкування, яка порушує комунікативну атмосферу. Найчастіше учасник-провокатор пише провокативні пости, дає різкі відповіді на зауваження, не підтримує ввічливої розмови, ухиляється від чесної відповіді.

3. Часом перебування в спільноті:

– постійний учасник-провокатор – учасник віртуальної спільноти, який часто та в різних розділах віртуальної спільноти чинить провокативні дії;

– «тематичний» учасник-провокатор – учасник віртуальної спільноти, який створює провокативні дії тільки в певному розділі. Цей учасник може залишити у віртуальній спільноті лише одне повідомлення, викликавши ним негативну реакцію інших учасників спільноти.

Для ідентифікації та уникнення учасників-провокаторів та запобігти даній проблемі можна декількома способами. «Вручну» – модератор сам відслідковує учасників-провокаторів та виконує дії

по їхньому усуненню з спільноти. За допомогою встановлення додатків з виявлення учасника-провокатора за ключовими словами, які несуть негативний характер. Застосування модератором методології та рекомендацій щодо виявлення тролів, програми розробленої групою дослідників Стенфордського і Корнельського університетів, яка призначена як допоміжний інструментарій для модераторів віртуальних спільнот [10]. Часто учасники-прово-катори створюють фейкові акаунти (з неправдивою контактною інформацією), для запобіганням таким учасникам необхідно застосовувати інструментарії з перевірки особи (наприклад, «Hoverme», «Identify», «Pipl.com», «Spokeo», «WebMii»).

Усунення флеймерів. Заходи захисту з усунення флеймерів полягають у виявлені та блокуванні учасників-флеймерів. Флейм – дискусія в якій учасники спільноти переходять від звичайної та початкової теми до особистих образ, суперечок та сварок. Учасників, які поширюють флейм, називають флеймерами. Поява філеймерів у віртуальній спільноти веде до конфліктів між учасниками. Найчастіше це стається на основі розбіжностей політичних, релігійних, соціальних та національних поглядів. Що призводить до появи частки негативно налаштованої аудиторії віртуальної спільноти.

У віртуальній спільноті варто виокремити два типи учасників-флеймерів: учасник, який сам стверджує про флейм; інші учасники чи модератор спільноти помітили флейм.

Для забезпечення захисту віртуальної спільноти від учасників-флеймерів адміністратору та модератору віртуальної спільноти необхідно виявляти учасників-флеймерів за допомогою наявних досліджених лінгвістичних особливостей текстів та лінгво-комунікативних індикаторів. Аналогічно до учасників-провокаторів флеймери створюють фейкові акаунти (з неправдивою контактною інформацією), для запобіганням таким учасникам-флеймерам необхідно застосовувати інструментарії з перевірки особи.

Запобігання Кібербулінгу. Цей метод протидії полягає у виявлені кібербулінгу. Кібербулінг – це дії спрямовані на переслідування осіб з використанням Інтернету та засобів електронної техніки. Найчастіше кібербулінг застосовують з метою приниження, ображення чи переслідування інших учасників віртуальної спільноти. Поява такого учасника негативно налаштовує інших користувачів віртуальної спільноти та несе за собою негативні наслідки. Наприклад, у спільноті з'являється учасник чи група учасників, які публічно цькують, переслідують та обмовляють іншого учасника спільноти.

Заходи захисту від кібербулінгу у віртуальній спільноті варто вжити у вигляді уточнення в правилах спільноти та виявлення учасників шляхом наявних рекомендацій з виявлення учасників-шкідників. Учасники-шкідники, аналогічно до провокаторів та флеймерів, створюють фейкові акаунти (з неправдивою контактною інформацією), для запобіганням таким учасникам необхідно застосовувати інструментарії з перевірки особи.

Показник входження віртуальної спільноти в зону ризику появи негативно налаштованої аудиторії віртуальної спільноти, основою для визначення даного показника частки шкідливих учасників (2):

$$NegativeAud^{(User)} = (1 - w_{\Pr} * \frac{Quantity(\Pr ovocateur^{(User)})}{Quantity(Common^{(User)})} + w_F * \frac{Quantity(Flame^{(User)})}{Quantity(Common^{(User)})} + w_K * \frac{Quantity(Cyberbullying^{(User)})}{Quantity(Common^{(User)})}), \quad (2)$$

де $\{w_{\Pr}, w_F, w_K\} \in W$ – вагові коефіцієнти кожного індикатора відповідно, визначаються менеджером організації життєвого циклу віртуальної спільноти, $0 \geq w_i \leq 1$, $w_i \in W$, $\sum_{w_i \in W} w_i = 1$; Quantity (Provocateur(User)) – кількість учасників-провокаторів у віртуальній спільноті; Quantity (Flame(User)) – кількість учасників-флеймерів у віртуальній спільноті; Quantity (Cyberbullying(User)) – кількість учасників, що займаються кібербулінгом у віртуальній спільноті; Quantity (Common(User)) – загальна кількість учасників віртуальної спільноти.

Зниження якості інформаційного наповнення. Суть ризику зниження якості інформаційного наповнення полягає в тому, що у віртуальній спільноті знижується рівень достовірності, грамотності та якості інформаційного наповнення. До інформаційного наповнення віртуальних спільнот віднесемо пости та коментарі. До заходів захисту від ризику зниження якості контенту належать: покращення якості інформаційного наповнення; покращення достовірності інформаційного наповнення; покращення рекламних оголошень.

Покращення якості інформаційного наповнення. Захід захисту перевірки якості інформаційного наповнення полягає в уточненні в правилах в частині вимог до інформаційного наповнення. Введення правил публікації повідомлень та коментарів у віртуальній спільноті.

Також важливою складовою якісного інформаційного наповнення є запобігання флуду, офтопіку, вайпу, оверквотингу , тобто нетикету (Інтернет етикету спілкування). Флуд – це повідомлення чи коментар в змісті якого немає ніякої корисної чи актуальної інформації. Офтопік – це повідомлення чи коментар, яке не стосується тематики віртуальної спільноти чи повідомлення. Вайп – створення нових безглуздих дискусії, для перенесення актуальної інформації вниз сторінки. Оверквотинг – завеликий розмір цитати, що є некомфортним для сприйняття [11]. Ще однією складовою якісного інформаційного наповнення є грамотно та легко для сприйняття написаний пост.

Заходами захисту є постійний моніторинг адміністратора та модератора віртуальної спільноти для виявлення перелічених вище складових нетикету. Застосування системи управління інформаційним наповненням (cms-системи). Також, одним з варіантів для покращення якості інформаційного наповнення є залучення зовнішніх копірайтерів.

Покращення достовірності інформаційного наповнення. Суть заходів захисту достовірності інформаційного наповнення полягає у перевірці на

достовірність інформаційного наповнення, що публікується у віртуальній спільноті. Дані заходи необхідні для запобігання фейковій (неправдивій) інформації, яка може спричиняти паніку серед учасників спільноти, маніпуляції, розпалювання ворожнечі між учасниками спільноти, заплямовувати чиюсь репутацію та ін.

Для захисту віртуальної спільноти від фейкової інформації існує безліч сервісів та додатків для перевірки достовірності інформаційного наповнення, як текстової інформації так і мультимедійної. Сервіси для перевірки зображень: Findexif.com, Foto Forensics, Google Search by Image, JeffreyвЂ™s Exif Viewer, JPEGSnoop, TinEye. Сервіси для перевірки текстової інформації: Snopes.com, PeopleBrowsr, HuriSearch, Geofeedia, Verify.org,ua, Lazy Truth, Trooclick, та ін.

Покращення рекламних оголошень. Суть заходів захисту перевірка рекламних оголошень полягає у відслідковуванні щоб в спільноту не потрапляла реклама, яка обурюватиме учасників чи не відноситиметься до змісту та діяльності віртуальної спільноти. Також, надмірна кількість рекламних оголошень перевантажує віртуальну спільноту порушуючи комунікативну атмосферу.

До заходів захисту спільноти від надмірної реклами належить застосування механізму інтернет-реклами – таргетинг, регулювання рекламних повідомлень відносно учасників. Заборона на рекламні оголошення створені учасником віртуальної спільноти. Показник входження віртуальної спільноти в зону ризику зниження якості інформаційного наповнення віртуальної спільноти (3):

$$InfContent^{(Inf)} = w_{Con} * \frac{Quantity(BadContent^{(Inf)})}{Quantity(Common^{(Inf)})} + w_{Cer} * \frac{Quantity(BadCertaint y^{(Inf)})}{Quantity(Common^{(Inf)})} + w_{Bl} * \frac{Quantity(Blurb^{(Inf)})}{Quantity(Common^{(Inf)})}, \quad (3)$$

де $\{w_{Con}, w_{Cer}, w_{Bl}\} \in w$ – вагові коефіцієнти кожного індикатора відповідно, визначаються менеджером організації життєвого циклу віртуальної спільноти, $0 \geq w_i \leq 1$, $w_i \in w$, $\sum_{w_i \in w} w_i = 1$; Quantity(Content(Inf)) – кількість неякісного інформаційного наповнення, оформленого не за правилами віртуальної спільноти; Quantity(Certaintity(Inf)) – кількість недостовірного інформаційного наповнення у віртуальній спільноті; Quantity(Blurd(Inf)) – кількість негативної реклами у віртуальній спільноті; Quantity(Common(Inf)) – загальна кількість інформаційного наповнення віртуальної спільноти.

Антизаконні матеріали та діяльність спільноти. Суть ризику полягає в тому, що у віртуальній спільноті з'являється інформаційне наповнення, яке не відповідає чинному законодавству, що несе за собою кримінальну відповідальність. До заходів захисту від ризику антизаконні матеріали та діяльність спільноти належать: правова верифікація; уникнення плагіату; запобігання фішингу.

Правова верифікація. Суть протидії полягає в уточненні в правилах віртуальної спільноти щодо діяльності та інформаційного наповнення спільноти відповідно до чинного законодавства. Недотримання даних правил віртуальної спільноти несе за собою притягнення до кримінальної відповідальності. Необхідно запобігти (уникати) інформаційному наповненню віртуальної спільноти, що містить інформацію з обмеженим доступом (конфіденційна, службова, особиста) (згідно Закону України «Про інформацію»), матеріали заборонені законом, віруси та ін.

Уникнення плагіату. Суть протидії полягає у відслідковуванні та забороні публікації інформаційного наповнення, яке містить ознаки плагіату. Згідно закону України «Про авторське право та суміжні права» плагіат – це оприлюднення (опублікування), повністю або частково, чужого твору під іменем особи, яка не є автором цього твору. Інформаційне наповнення в мережі Інтернет (текст, графічне зображення, аудіо- та відео- файли) є об'єктами авторських прав, за винятком матеріалів, що зазначені в ст.10 Закону України «Про авторське право та суміжні права». За недотримання авторських та суміжних прав передбачена кримінальна відповідальність, що несе загрозу репутації та діяльності віртуальної спільноти [11-12]. Для запобігання публікації інформаційного наповнення, яке містить ознаки плагіату, перед публікацією у віртуальній спільноті модератору варто застосовувати антиплагіатні програми (наприклад, StrikePlagiarism.com, Etxt-Антиплагиат (AntiPlagia-rasm.net), ПЗ «AdvegoPlagiatus 1.3.1.7» та ін.).

Запобігання фішингу. Даний метод полягає в захисті особистої інформації та конфіденційних даних користувачів віртуальної спільноти та запобіганні фішингу. Фішинг – це виманювання (незаконне одержання) персональних даних учасників віртуальної спільноти.

Показник входження віртуальної спільноти в зону ризику антизаконного інформаційного наповнення та діяльності віртуальної спільноти (4), де $\{w_{Cr}, w_{Pl}, w_{Ph}\} \in w$ – вагові коефіцієнти кожного індикатора відповідно, визначаються менеджером організації життєвого циклу віртуальної спільноти, $0 \geq w_i \leq 1$, $w_i \in w$, $\sum_{w_i \in w} w_i = 1$; Quantity(Crime(Inf)) – кількість інформаційного наповнення віртуальної спільноти, що не відповідає чинному законодавству; Quantity(Plagiarism(Inf)) – кількість інформаційного наповнення віртуальної спільноти з вмістом плагіату; Quantity(Common(Inf)) – загальна кількість інформаційного наповнення віртуальної спільноти; Quantity(Phishing(User)) – кількість користувачів віртуальної спільноти, які чинять фішингові дії; Quantity(Common(User)) – загальна кількість користувачів віртуальної спільноти:

$$AntiLegal = 1 - (w_{Cr} * \frac{Quantity(Crime^{(Inf)})}{Quantity(Common^{(Inf)})} + w_{Pl} * \frac{Quantity(Plagiarism^{(Inf)})}{Quantity(Common^{(Inf)})} + w_{Ph} * \frac{Quantity(Phishing^{(User)})}{Quantity(Common^{(User)})}), \quad (4)$$

Втрата контролю над спільнотою. Суть ризику полягає в тому, що модератор може втратити контроль над керуванням віртуальною спільнотою.

До заходів захисту від ризику втрати контролю над спільнотою належать: формування лідера спільноти; керування лідером спільноти. ***Формування лідера спільноти.*** Суть захисту полягає у формуванні учасника-лідера та керуванні ним в свою користь. ***Керування лідерами спільноти.*** Суть захисту полягає у виявленні лідерів у віртуальній спільноті та співпраці з ними.

Показник входження віртуальної спільноти в зону ризику втрати контролю над віртуальною спільнотою (5), де $\{w_{NL}, w_L\} \in w$ – вагові коефіцієнти кожного індикатора відповідно, визначаються менеджером організації життєвого циклу віртуальної спільноти, $0 \geq w_i \leq 1$, $w_i \in w$, $\sum_{w_i \in w} w_i = 1$; Quantity(NewLeader(User)) – кількість лідерів, створених адміністраторами спільноти; Quantity(Leader(User)) – кількість лідерів у віртуальній спільноті; Quantity(Common(User)) – загальна кількість учасників віртуальної спільноти:

$$Control^{(User)} = w_{NL} * (1 - \frac{Quantity(NewLeader^{(User)})}{Quantity(Common^{(User)})}) + w_L * \frac{Quantity(Leader^{(User)})}{Quantity(Common^{(User)})}, \quad (5)$$

Алгоритм визначення рівня інтенсивності заходів протидії соціально-орієнтованим ризикам. Алгоритм розроблений з метою впровадження запропонованих заходів захисту віртуальної спільноти від соціально-орієнтованих ризиків, зображений на рис. 1.

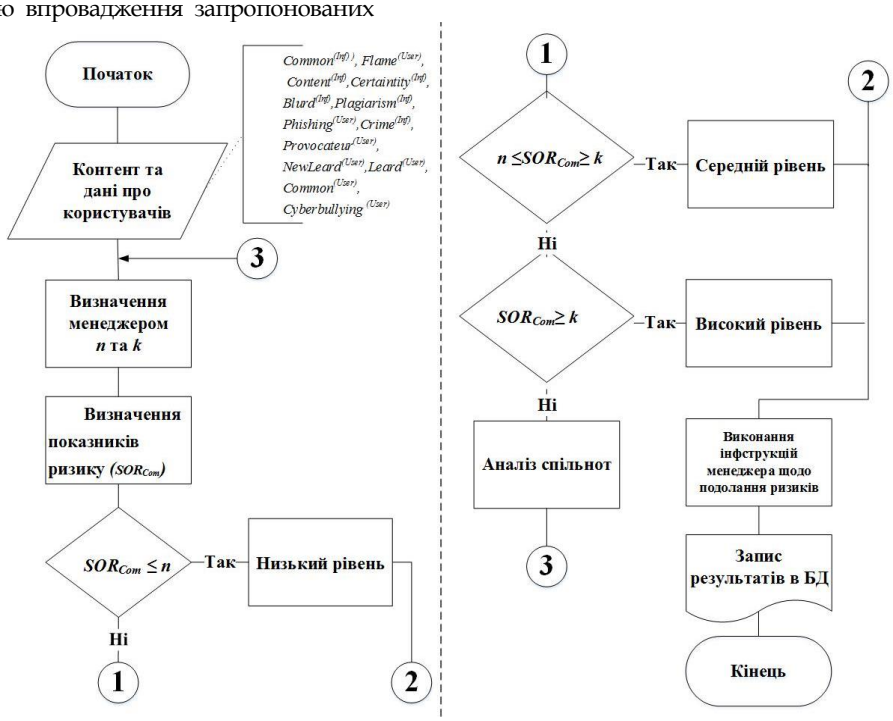

Рис. 1. Алгоритм визначення рівня інтенсивності заходів протидії соціально-орієнтованим ризикам

Вхідними даними для алгоритму є: Provocateur(User) – учасники-провокатори віртуальної спільноти; Flame(User) – учасники-флеймери віртуальної спільноти; Cyberbullying(User) – учасники, що займаються кібербулінгом у віртуальній спільноті; Content(Inf) – неякісне інформаційне наповнення у віртуальній спільноті; Certaintity(Inf) – недостовірне інформаційне наповнення у віртуальній спільноті; Blurd(Inf) – негативна реклама у віртуальній спільноті; Plagiarism(Inf) – інформаційне наповнення віртуальної спільноти з вмістом плагіату; Crime(Inf) – інформаційне наповнення, що не відповідає чинному законодавству; Phishing(User) – користувачі віртуальної спільноти, що потрапили під дію фішингу; NewLeader(User) – лідери віртуальної спільноти, створені адміністраторами; Leader(User) – лідери віртуальної спільноти.

Результатом реалізації алгоритму є класифікація рівня ризику: 1. Високий рівень (Ind ≤ n, n визначається менеджером організації життєвого циклу віртуальної спільноти). При високому рівні входження показника в зону ризику необхідно провести аналіз спільноти (завдання для аналітика) та визначити прогалини у організації життєвого циклу віртуальної спільноти. 2. Середній рівень (n ≤ Ind ≥ k, n та k визначаються менеджером організації життєвого циклу віртуальної спільноти). При середньому рівні входження показника в зону ризику необхідно вжити заходів протидії соціально-орієнтованим ризикам. 3. Низький рівень (Ind ≥ k, k визначаються менеджером організації життєвого циклу віртуальної спільноти). При низькому рівні входження показника в зону ризику спільнота може повноцінно функціонувати.

Висновки

Запропоновані у статті соціально-орієнтовані ризики організації життєвого циклу віртуальної спільноти дозволяють забезпечити якісний загальний стан виконання проекту створення віртуальної спільноти. Визначення рівня входження спільноти в зону ризику пришвидшить виконання запропонова-

них заходів протидії соціально-орієнтованим ризикам організації життєвого циклу віртуальної спільноти. Застосування алгоритму визначення рівня інтенсивності заходів протидії соціально-орієнтованим ризикам є важливим для підвищення ефективності створення віртуальної спільноти та покращення процесу функціонування протягом усього її існування, забезпечення досягнення цілей та розвитку віртуальної спільноти.

Література

[1] О.Б. Данченко, І.А. Маклєв, Г.А. Баленко, «Методи та засоби аналізу проектних ризиків», *Вісн. Черкас.держ.технол.ун-т.*, Черкаси, ЧДТУ, № 1, с. 87-92, 2004.

[2] О.Б. Данченко, В.О. Занора, «Огляд методів аналізу ризиків в проектах», *Управління проектами та розвиток виробництва*, Луганськ, вид-во Східноукраїнський нац. ун-т ім. В. Даля, № 1(21), с. 57-64, 2007.

[3] D. Pimchangthong, V. Boonjing, «Effects of risk management practices on it project success», *Management and Production Engineering Review*, Т. 8, № 1, p. 30-37, 2017.

[4] О.Б. Данченко, «Огляд сучасних методологій управління ризиками в проектах», *Управління проектами та розвиток виробництва, зб.наук.пр.*, Луганськ, вид-во СНУ ім. В.Даля, №1(49), с. 16-25, 2014.

[5] A. McNeil, R. Frey, P. Embrechts, «Quantitative risk management: concept, techniques and tools», *Princeton University Press*, p.699, 2015.

[6] R.H. Ansah, S. Sorooshian, S.Bin Mustafa, O.S. Oludapo, «Constructions Project Management Risks' Framework», *Quality-Access to Success*, Т. 18, № 158, с. 90-95, 2017.

[7] C. Muriana, G. Vizzini, «Project risk management: A deterministic quantitative technique for assessment and mitigation», *International Journal of Project Management*, Т. 35, № 3, p. 320-340, 2017.

[8] О.Р Трач, «Соціально-орієнтовані ризики при організації життєвого циклу віртуальної спільноти», *Інформаційна діяльність, документознавство, бібліотекознавство: історія, сучасність, перспективи, матеріали III Всеукр. наук.-практ. конф.*, Київ, с. 40-44, 2017.

[9] Н. Романенко, Я. Михайлишин, П. Солодько, О. Зог, «Тролосфера». [Електронний ресурс]. Режим доступу: http://texty.org.ua/d/fb-trolls/.

[10] А.М. Пелещишин, Ю.О. Сєров, К.О. Слобода, «Виявлення та усунення конфліктів між учасниками спільнот середовища Веб 2.0 на прикладі Веб-форумів», *Східно-Європейський журнал передових технологій*, Харків, №6/3 (42), с. 55–59, 2009.

[11] A. Peleshchyshyn, Z. Holub, «Development of the System for Detecting Manipulation in Online Discussions», *SCIT 2016: Recent Advances in Systems, Control and Information Technology*, pp. 111-117.

[12] Про авторське право і суміжні права, Закон України: від 23.12.1993 р., No 3792-XII. [Електронний ресурс]. Режим доступу : http:\\rada.gov.ua.

[13] П.С Ріппа., «Забезпечення авторських прав у мережі Інтернет». [Електронний ресурс]. Режим доступу: http://www.nbuv.gov.ua

УДК 004.773.2 (045)

Пелещишин А.Н., Трач О.Р. Определение элементов социально-ориентированных рисков при организации жизненного цикла виртуальных сообществ

Аннотация. *В статье предложены социально-ориентированные риски при организации жизненного цикла виртуального сообщества, а именно: риск появления негативно настроенной аудитории, риск снижения качества информационного наполнения, риск антизаконных материалов, риск потери контроля над сообществом. Исследуемым элементом социально-ориентированных рисков является текстовое информационное наполнение, включающее комментарии и посты в виртуальном сообществе. Предложенные меры по противодействию социально-ориентированным рискам, а именно: избежание участников провокаторов, устранение флеймерив, предотвращение Кибербуллингу, улучшение качества информационного наполнения, улучшение достоверности информационного наполнения, улучшение рекламных объявлений, правовая верификация, во избежание плагиата, предотвращение фитингов, формирования лидера сообщества, управление лидером сообщества. Представленное определение показателя вхождения сообщества в зону социально-ориентированного риска. Разработан алгоритм определения уровня интенсивности мер противодействия социально-ориентированным рискам. Осуществлена классификация уровня рисков на высокий, средний и низкий уровни.*

Ключевые слова: *виртуальное сообщество, риск, жизненный цикл, участники, информационное наполнение.*

Peleshchyshyn A., Trach O. Determination of elements of socio-oriented risks by organization of the life cycle of the virtual community

Abstract. *The article proposes socially-oriented risks in the organization of the life cycle of the virtual community, namely: the risk of negative audience appearance, the risk of lowering the quality of information content, the risk of illegal materials, the risk of loss of control over the community. The exploratory element of socially-oriented risk is a text informational content that includes comments and posts in the virtual community. Proposed measures to counteract socially-oriented risks, namely: avoiding participants of provocateurs, eliminating flames, preventing cybersquatting, improving the quality of information content, improving the reliability of information content, improving adverts, legal verification, avoiding plagiarism, preventing fitting, forming a community leader, managing Community leader. The definition of the index of the community's entry into the socially-oriented risk zone is presented. An algorithm for determining the level of intensity of measures to counteract socially-oriented risks has been developed. Classification of the level of risk at high, medium and low levels has been carried out.*

Key words: *virtual community, risk, life cycle, participants, content.*

Отримано *17 червня 2017 року*, затверджено редколегією *18 липня 2017 року*