УДК 338.054.23

О. Є. Кузьмін, Н. С. Станасюк, Д. А. Берднік
Національний університет "Львівська політехніка"

ПРИКЛАДИ РЕЗУЛЬТАТІВ ВІД ДІЇ НЕГАТИВНИХ СЦЕНАРІЇВ ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

http://doi.org/10.23939/smeu2019.02.018

Наведено приклади широко відомих випадків настання ризиків, пов'язаних із негативними сценаріями використання програмного забезпечення, що спричинили вагомі втрати власників, авторів чи суспільства. Основним критерієм для пошуку та вибору таких прикладів стали достовірність, вагомість та можливість подати точні дані про економічні втрати або порядок втрат. Висвітлено основні передумови настання ризику, перебіг подій та втрати, що стали наслідком. Проведено оцінювання економічного результату подій. Запропоновано підхід до оцінювання значущості втрат.

Ключові слова: негативні сценарії; економічний результат; втрати; розроблення програмного забезпечення.

Постановка проблеми

Як інструмент для описання роботи програмного забезпечення використовують створення позитивних сценаріїв використання додатків, так званих "історій користувачів". Під позитивним сценарієм розуміють певну послідовність дій користувача, що неодмінно приводить до виконання бізнес-функції додатка та досягнення бізнес-мети, яку ставить використання цього програмного забезпечення. Розглядаючи приклад CRM[1]-системи, можна припустити таку історію користувача: "Як спеціаліст із продажу продукції, я хочу ввести дані можливого клієнта в базу даних". Перша частина сценарію (до коми) вказує на конкретного користувача, а друга на бізнес-функцію, яку він має виконати за допомогою описуваного додатка. За допомогою множини позитивних сценаріїв повністю визначається бізнес-мета програмного забезпечення для його подальшого розроблення.

Натомість негативними сценаріями називають такі дії користувача, які не приводять до виконання бізнес-функції додатка (або призводять до некоректного виконання) і, як наслідок, не ведуть до досягнення бізнес-мети. Однак важливо розуміти, що на додачу такі сценарії можуть спричинити додатковий негативний результат. У деяких випадках такий негативний результат може зумовити значні економічні наслідки. Розуміння рівня таких втрат має критичне значення для прийняття рішення щодо інвестування у блокування таких сценаріїв.

У низці випадків практично корисно під час прийняття рішень розглянути приклад випадку, що стався в аналогічній галузі або в процесі використання аналогічного програмного забезпечення. Такі приклади допомагають зрозуміти, що існують сфери сучасного бізнесу, пов'язані зі значним ризиком вагомих втрат. І навіть більше, в деяких випадках можливо знайти приклади, що описують не тільки аналогічну сферу, а й аналогічні бізнес-цілі додатка.

Актуальність дослідження

Важливим аспектом сучасного планування проєктних робіт є формування множини негативних сценаріїв, що необхідно врахувати. Як правило, для прийняття рішення щодо необ-

[1] Client Relationship Management systems.

хідності блокування того чи іншого негативного сценарію враховують оцінку можливих економічних наслідків, його реалізації та вірогідність настання такого сценарію або порівняння із втратами, яких зазнали, розробляючи аналогічні додатки чи додатки в аналогічній сфері.

Отже, одна із цілей розроблення сучасного програмного забезпечення – блокувати виконання негативних сценаріїв чи попередити про можливі наслідки. Таку ціль досягають за два основні етапи. По-перше, розробляючи технічну документацію до проєкту, опрацьовують типові або специфічні для області застосування негативні сценарії із метою виявлення критичних ризиків та розроблення елементів програмного забезпечення, що блокуватиме виконання таких сценаріїв. По-друге, під час перевірки якості програмного забезпечення перевіряють і негативні сценарії.

Формулювання мети та завдань статті

Основна мета цієї роботи – обґрунтувати необхідність врахування негативних сценаріїв використання програмного забезпечення під час його розроблення; надати спеціалістам із управління ризиками, менеджерам проєктів із розроблення програмного забезпечення та науковцям, що працюють над розвитком наукового підґрунтя управління ризиками, структурований матеріал для класифікації та оцінювання ризиків та економічного результату від їх настання за допомогою історичних аналогів.

Аналіз останніх досліджень і публікацій

Зазначимо, що загальний підхід до розгляду ризиків під час впровадження нововведень розглянуто у роботі [1]. Крім того, деякі вчені розглядають конкретні випадки втрат від певних негативних сценаріїв використання програмного забезпечення, зосереджуючись на деталях та перебігу подій в межах одного інциденту. Такі роботи надають повну інформацію про певну подію, а також оцінку автора щодо неї, її причин та наслідків. Яскравими прикладами таких робіт є: роботи Troy Gallagher [2] та Kimberley Chong [3], що досліджували інцидент із апаратом Therac 25, робота Douglas Arnold [4], що детально висвітлив інцидент із ракетою “Патріот”, а також праця Darren Dalcher[5], який ретельно дослідив колапс лондонської системи невідкладної допомоги. Однак роботи із порівнянням низки інцидентів у контексті впливу негативних сценаріїв використання програмного забезпечення знайти не вдалося.

Виклад основного матеріалу

Для з’ясування дії негативних сценаріїв використання програмного забезпечення на основі прикладів із різних сфер сучасного бізнесу розглянемо кілька випадків. Їх економічний результат проаналізуємо за такими класами втрат (якщо вони були): незворотні втрати, втрати інформації, втрати операційного часу, репутаційні втрати. Для кожного випадку буде підрахований повний економічний результат.

Некоректна робота апарата Therac 25. Цей апарат розробив підрозділ[2] канадської державної компанії Atomic Energy of Canada Limited (далі AECL) у 1982 р. як продовження успішної моделі Therac 20. Його використовували для комплексної променевої терапії [6]. Як виявилось згодом, упродовж 1985–1987 рр. специфічний сценарій використання цього апарата спричинив щонайменше шість випадків важкої променевої хвороби у пацієнтів, що отримували променеву терапію [2]. Достеменно відомо, що двоє з них загинуло саме від наслідків променевої хвороби. Вагомість негативного впливу апарата Therac 25 як основної причини смерті інших постраждалих можна поставити під сумнів з огляду на їхній стан на момент початку терапії.

Цей випадок є показовим з кількох причин. По-перше, з усієї серії апаратів Therac саме Therac 25 вперше мав тільки електронний, а не механічний захист від надмірного опромінення. Тобто йдеться про значний інцидент з погляду зони відповідальності програмного забезпечення. По-

[2] Як окрема організація відомий під назвою “Radiochemical Company”.

друге, аналіз причин виникнення передумов інцидентів показує, що через організаційні недоліки увагу не приділено передусім негативним сценаріям, інтеграційним сценаріям апаратної та програмної складових, а також що загальний рівень перевірки як сценаріїв використання програмного продукту, так і усього апарата був низьким. Незважаючи на ризикований та амбітний крок – відмову від механічного контролю за радіаційною безпекою, що мав би ініціювати розроблення нового програмного забезпечення, для Therac 25 використано модифіковану програмну компоненту апарата Therac 20, який мав механічний захист. Саме наявність механічного захисту від надмірного опромінення блокувала альтернативний сценарій, що став причиною інцидентів.

Оцінюючи економічні наслідки, необхідно звернути увагу саме на людські жертви, оскільки фінансові втрати компанії були частково або повністю покриті страховками і наявність позовів із боку жертв або їх родичів у всіх випадках сумнівна [3]. Отже, до уваги можна брати лише еквівалентну вартість людського життя, як показано в роботі [7]:

$$\sum_d = L_e V = \$9M \times 6 = \$54M,$$

де $\sum_d$ – сума економічних втрат, пов'язаних із загибеллю людей; L_e – економічний еквівалент вартості людського життя; V – кількість можливих учасників групового позову (жертв).

Також відомо про заборону на використання продуктів компанії з 1991 до 1994 [8] рр., хоча вона була повною лише впродовж 1991 р. і аж до повної відміни залишалась частковою. Точні економічні показники унаслідок втрат операційного часу встановити важко, адже немає точних даних про недоотриманий прибуток.

Економічний результат від репутаційних втрат можна відстежити, аналізуючи подальший розвиток підрозділу Radiochemical Company. Підрозділ продано як окрему компанію у 1988 р. [9]. Передусім треба розуміти, що поспіх, із яким підрозділ було приватизовано та продано[3] приватним інвесторам, свідчить про те, що компанія AECL, яка передусім спеціалізується на устаткуванні для атомної енергетики, прагнула зменшити репутаційний вплив на свій основний бізнес. Однак за фактом цієї угоди канадському уряду довелося виплатити декілька компенсацій [9]:

1. Пряму виплату в розмірі $5M.
2. Безвідсотковий займ на $100M (без розкриття терміну та умов повернення).
3. Виплату $12,5M від імені компанії AECL.

Потрібно також додати ще й знижку на $14,5M, надану під час продажу. Компанія AECL, безперечно, зіткнулася зі значними ринковими наслідками репутаційних втрат і зниженням довіри до її продуктів. Точний економічний результат встановити важко, оскільки ані компанія AECL, ані її підрозділ не публікували публічних звітів на час інциденту. Однак достеменно відомо про повернення принаймні шести апаратів. Із урахуванням їх вартості втрати компанії мали сягнути $18M[4]. Загалом, відкидаючи займ через неможливість обчислити недоотриманий прибуток Канади, репутаційні втрати, спричинені інцидентом, можна виразити як:

$$\sum_r = M_r + R_r + L_r = \$3M \times 6 + \$5M + \$12{,}5M + \$14{,}5M = \$50M,$$

де $\sum_r$ – сума економічних втрат, пов'язаних із репутаційними втратами; M_r – об'єми ринку, що втрачено внаслідок репутаційних втрат; R_r – витрати на відновлення репутації; L_r – інші економічні наслідки від репутаційних втрат.

Отже, загальні втрати ($\sum_{\text{заг.}}$) можуть сягати:

$$\sum_{\text{заг.}} = \sum_d + \sum_r = \$54M + \$50M = \$104M.$$

Похибка системи наведення ЗРК "Патріот". Під час війни у Перській затоці для оборони певних військових об'єктів коаліції [6] та мирних жителів на території Саудівської Аравії було розгорнуто батарею зенітно-ракетних комплексів (ЗРК) "Патріот"[5], які повинні були здійснювати перехоплення ракет класу земля–земля, випущених військами Іраку. Характеристики ЗРК, а також

[3] Під назвою Nordion International Inc.

[4] Середня ціна такого апарата становить приблизно $3M.

[5] Зенітно-ракетний комплекс MIM-104 Patriot.

диспозиція дозволяли перехопити всі можливі цілі, що міг використати противник. Однак 25 лютого 1991 р. ракета SCUD[6] влучила у барак із військовослужбовцями армії США. Внаслідок прямого попадання загинуло 28 бійців та близько 100 були поранені. Ракета "Патріот", випущена на перехоплення, не влучила у ціль [4].

Аналіз інциденту показав, що старт ракети було зареєстровано коректно і часу підльоту було достатньо для реагування та ефективного перехоплення. Як зазначено в офіційному звіті [10], перехоплення не вдалось через похибку в розрахунку часу підльоту ракети супротивника. Програма управління комплексом містила методи, що визначали час у частках секунди із похибкою. Ця похибка була незначна і під час стандартних випробувань не давалася взнаки, але під час безперервної роботи впродовж більш як 20 годин спричиняла помилку наведення, більшу за зону контакту (фактичний проліт повз). На момент інциденту комплекси були на бойовому чергуванні орієнтовно 100 годин. Основною причиною цієї проблеми було те, що сама по собі похибка була замалою для того, щоб справляти значущий вплив (та бути виявленою під час випробувань), але вона мала акумулятивний ефект, який можна виявити лише упродовж довгострокових випробувань. Нестандартний час роботи є одним із типових негативних сценаріїв використання програмного забезпечення і нині широко використовується для моделювання роботи важливих систем.

Розглядаючи наслідки трагедії, варто звернути увагу на кількість жертв, що є надвеликою навіть із огляду на стан війни. Згідно із законодавством США загибель або скалічення військовослужбовців гарантує виплати постраждалим або їх родичам. Враховуючи розмір мінімальної виплати [11], можна припустити, що Міністерство оборони зазнало збитків на $2,8M лише за виплатами загиблим. Точний розмір виплат пораненим встановити важко, оскільки відсутні публічні дані про ступінь поранень та втрату працездатності через них.

Втрати від знищення військового майна не розголошують. Однак у доступних джерелах згадано про знищення барака (важливіші об'єкти військового майна не вказано).

Отже, незворотні втрати можна розрахувати як:

$$\sum_d = L_e V + V B_g = \$9M \times 28 + \$100\,000 \times 28 = \$254{,}8M,$$

де $\sum_d$ – сума економічних втрат, пов'язаних із загибеллю людей; L_e– економічний еквівалент вартості людського життя; V – кількість можливих учасників групового позову (жертв); B_g – сума компенсації.

Як зазначають багато експертів, інцидент спричинив значний рівень недовіри до цих комплексів, але, на жаль, з огляду на об'єктивні причини неможливо відстежити динаміку подальших продажів чи частку ринку. Однак історія цін на акції компанії Raytheon[7], що є виробником комплексу, доступна у публічних джерелах [12].

Аналіз історії біржових торгів щодо цього асету показав, що у період інциденту (рис. 1), а також у період публікації звіту (рис. 2) визначних трендових падінь не відбувалося. Отже, встановлено, що вплив інциденту на загальні показники компанії виробника відсутній або незначний.

Оскільки неможливо встановити, чи були втрати цінних даних, а також втрати операційного часу, економічний результат ($\sum_{\text{заг.}}$) від інциденту (який можна обчислити за наявних даних) дорівнює економічному результату від незворотних втрат, а саме:

$$\sum_{\text{заг.}} = \sum_d = \$254{,}8M.$$

Колапс системи розподілення карет швидкої допомоги міста Лондон є одним з найпоказовіших з огляду на масштаб, кількість проблем і широке обговорення у пресі, офіційних

[6] Мобільний оперативно-тактичний ракетний комплекс 9К72 "Ельбрус", за класифікацією НАТО – SS-1c/b/e SCUD-B/C/D.

[7] NYSE: RTN.

звітах [13] та наукових роботах з управління ризиками, якістю та проєктами. London Ambulance Service [6] (LAS), що є фактичним підрозділом національної служби охорони здоров'я Англії, 26 жовтня 1992 року зробила спробу перейти на електронну систему розподілення карет швидкої допомоги [5]. Цей крок спричинив колапс системи, що призвів до 46 смертей через ненадання невідкладної медичної допомоги [5]. Як свідчать звіти [13] та робота над помилками, причиною інциденту стали істотні помилки в організації проєкту, низька якість наданого програмного забезпечення, а також помилки в управлінні вимогами. З вищенаведених причин варто звернути увагу на те, що всі без винятку працівники служби швидкої допомоги (від операторів кол-центрів до медичного персоналу швидких) не брали участі у формуванні вимог до програмного комплексу, а також його прийманні. Тобто реальний практичний досвід не враховано, брали до уваги лише ідеальний перебіг подій без детального розуміння його етапів.

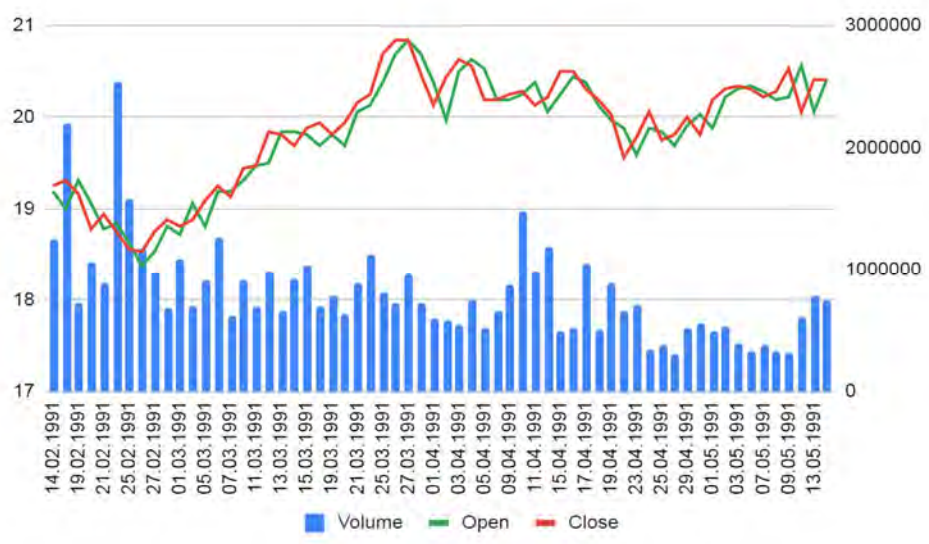

Рис. 1. Ціни асету RTN [12] впродовж трьох місяців після інциденту

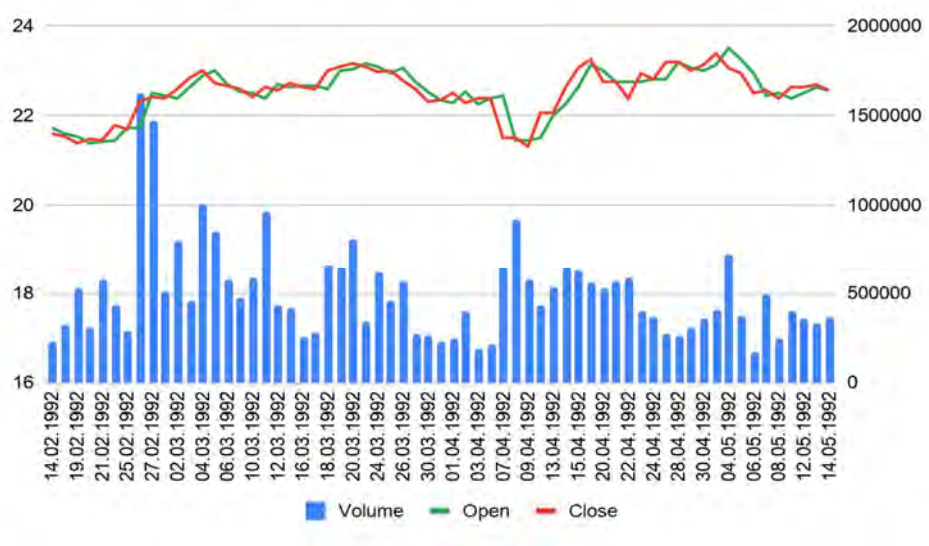

Рис. 2. Ціни асету RTN[12] впродовж трьох місяців після публікації звіту [10]

Приклади результатів від дії негативних сценаріїв використання програмного забезпечення

Для предмета цієї статті інтерес становлять саме негативні сценарії використання програмного забезпечення, які через помилки в управлінні вимогами не були враховані та справили значний негативний вплив на перебіг подій. Більшість авторів, які аналізували цей інцидент, наводять такі негативні сценарії, вплив яких став вирішальним:

1. Система не могла обробляти заявки на надання невідкладної допомоги, що не містили повної інформації про постраждалого, інцидент та багато іншої. Такий недолік спричинив великі затримки в оформленні звернень, а також значну кількість даних, що не відповідали дійсності й вводились лише для того, щоб система прийняла заявку.

2. Система не могла виявляти та обробляти дублі, й повторні виклики від людей, що не дочекалися швидкої, додавала до списку активних викликів, тому до тієї самої адреси направляла декілька карет.

3. У системі не була передбачена можливість редагувати створені виклики або коригувати помилково надані статуси.

4. Повідомлення про системні помилки виводилися разом із повідомленнями про виклики (не було можливості фільтрувати або вимкнути системні повідомлення). Через це за кілька годин термінали в каретах швидкої були фактично заблоковані й медичний персонал не мав змоги прийняти виклик.

5. Система не могла обробити неточну інформацію від модулів визначення місцезнаходження швидких. З цієї причини екіпажі, які на момент створення виклику рухалися або на модуль яких впливали радіоперешкоди (що доволі типово у великому місті), ігнорувалися і виклик передавали дуже віддаленим швидким.

6. Система не була технічно розрахована на перевантаження і мала технічні проблеми з перших годин роботи. Тести під навантаженням також не проводилися.

Оцінюючи економічний результат цієї події, варто звернути увагу насамперед на кількість пов'язаних з нею людських жертв. Використовуючи показники, запропоновані у роботі [7], виконаємо розрахунок:

$$\sum_d = L_e V = \$9M \times 46 = \$414M,$$

де $\sum_d$ – сума економічних втрат, пов'язаних із загибеллю людей; L_e – економічний еквівалент вартості людського життя; V – кількість можливих учасників групового позову (жертв).

Ця подія мала значний суспільний резонанс і вплинула як на державні органи, що відповідали за надання невідкладної допомоги, так і на приватні компанії, причетні до розроблення цього програмного продукту. Дарен Далчер у своїй оглядовій роботі [5] наводить список найвідоміших публікацій у ЗМІ світового значення. Чисті економічні втрати держави через зупинку проєкту становлять $1{,}5^8$ мільйонів фунтів [14]. Компанія-розробник System Options Limited одразу ж після трагічних подій втратила замовлення від національної пожежної служби і згодом була ліквідована через репутаційні втрати. Значних репутаційних втрат зазнала і LAS, що призвело до істотних кадрових змін, негативної суспільної думки та зменшення надходження державних коштів на реформування та вдосконалення. За деякими даними можна зробити висновок, що LAS продовжила розвиток лише у 2006 р. Беручи до уваги опубліковані числові показники, загальний результат від інциденту ($\sum_{заг.}$) можна подати як суму наведених вище втрат:

$$\sum_{заг.} = \$414M + \$2{,}65M = \$416{,}65M.$$

Втрата даних користувачів Sidekick. T-Mobile Sidekick (комерційна назва пристрою) або Danger Hiptop (базова назва пристрою) – це серія мобільних пристроїв, які розробила компанія Danger та пропонувала спільно із телекомунікаційною компанією T-Mobile USA на ринку Сполучених Штатів Америки. Орієнтовно від 29 вересня до 6 жовтня 2009 року компанія втратила особисті дані більш як 800 000 клієнтів [6].

[8] За курсом 1992 р. це становить приблизно $265000.

Однією із головних переваг цього пристрою була регулярна процедура копіювання даних користувача (адресна книга, дописи, фото, повідомлення, розклад тощо) на сервер компанії Danger. Продукт позиціонувався як унікальний інструмент, що надійно опікується даними користувача. Це було головною "обіцянкою" рекламної кампанії, отже, пряме порушення угод із користувачами є першим фактом, що виділяє цей випадок. По-друге, цей випадок є найбільшим прецедентом втрати даних хмарними сервісами, що й досі впливає на репутацію хмарних сервісів та довіру до них. По-третє, оскільки компанія Danger у 2008 р. була поглинута компанією Microsoft і на час інциденту це був структурний підрозділ компанії, цей випадок став одним з чинників негативного суспільного ставлення до аквізицій з боку Microsoft.

Програмне забезпечення, що контролює систему бекапів Sidekick, ігнорувало доволі вірогідний негативний сценарій, а саме втрату копії даних на хмарному сервері. В разі виходу із ладу сервера або втрати зв'язку із ним дані, що зберігалися на пристрої, вважалися недостовірними за замовчуванням. І навіть більше, під час перезавантаження пристрою дані на ньому видалялися автоматично, оскільки вважалися неактуальними, і мали бути завантаженими з сервера. Не можна було також скопіювати наявну на пристрої інформацію на інший носій або комп'ютер. Отже, після технічних проблем із серверним устаткуванням пристрої, що перезавантажувалися, видаляли всю наявну на них інформацію.

Варто врахувати, що інцидент не спричинив вагомих незворотних втрат, крім втрати інформації, що буде розглянуто окремо; втрати операційного часу через інцидент важко встановити, оскільки достеменно не відомо, які операційні можливості не були доступні. Отже, основними чинниками економічних втрат у цій події є втрати даних та репутаційні втрати.

Ключовим для розуміння збитків від втрати даних є груповий позов, поданий до компанії T-Mobile USA [15]. Ще до розгляду справи компанія надіслала постраждалим користувачам подарункові карти номіналом $100, які можна було використати для оплати послуг T-Mobile. Після розгляду справи їм було присуджено додаткові виплати (у формі послуг та контенту) в розмірі $34,88. Отже, збитки від втрати даних можна розрахувати як:

$$\sum_i = C_i V = (\$100 + \$34{,}88) \times 800\,000 = \$107{,}9M,$$

де $\sum_i$ – сума економічних втрат, пов'язаних із втратою інформації; V – кількість учасників групового позову, C_i – компенсація за умовами групового позову.

Для оцінювання репутаційних втрат варто звернути увагу на показники основних відповідачів за груповим позовом.

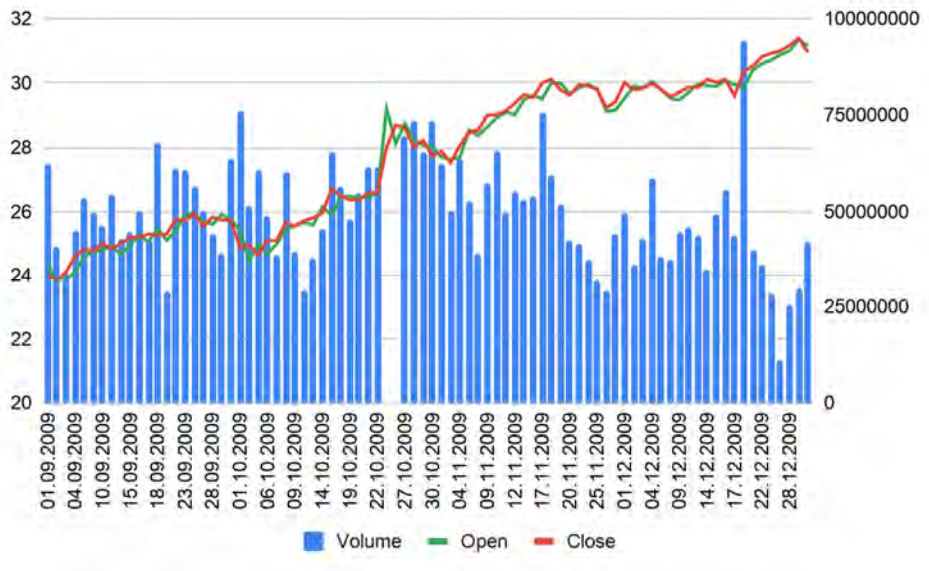

Рис. 3. Ціни асету MSFT від початку інциденту [12]

Акції компанії Microsoft[9] не зазнали помітних змін унаслідок описаних подій або публікації рішень суду (рис. 3). Таку відсутність реакції можна пояснити тим, що Danger, або Microsoft Azure[10] не мають окремого біржового індексу, тож MSFT відображає загальний інтерес до компанії та її продуктів, ураховуючи як проблемні активи, так і успішні.

Водночас виник довгостроковий тренд на здешевлення акцій компанії T-Mobile[11], що однозначно свідчить про негативний вплив на репутацію компанії (рис. 4).

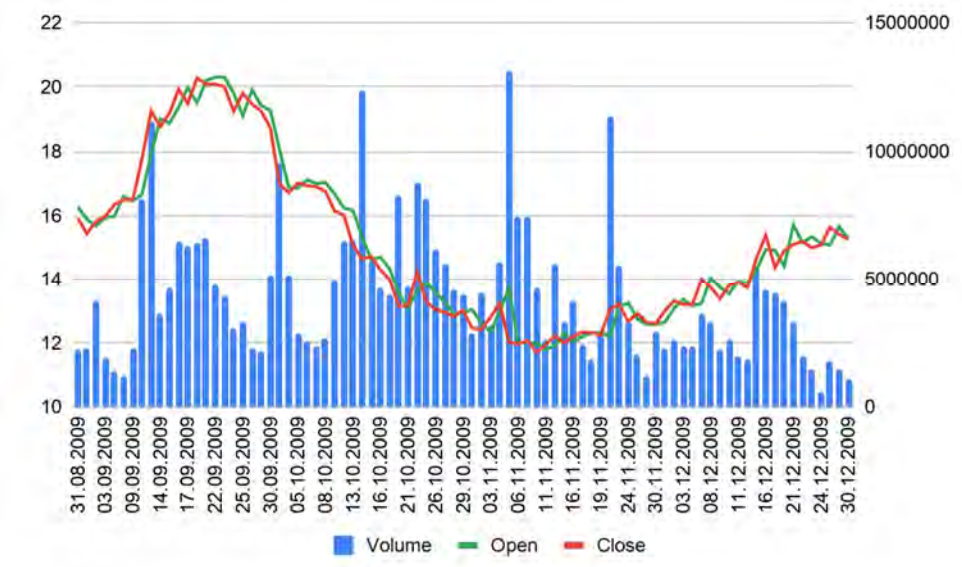

Рис. 4. Ціни асету TMUS на момент інциденту та після нього [12]

Розглянувши цей період детальніше, отримаємо графік, що надає дані для розрахунку економічних втрат.

Рис. 5. Детальна динаміка здешевлення асету TMUS після інциденту [12]

[9] NasdaqGS: MSFT.
[10] Хмарний сервіс від компанії Microsoft.
[11] NasdaqGS: TMUS.

Використовуючи ці дані, розраховуємо загальний обсяг втрат від здешевлення акцій компанії (витрати, які необхідно здійснити для відновлення початкової ціни асету). Як V_1–V_n приймаємо обсяги торгів акціями компанії, у період з 07.10.2009 р. до 11.11.2009 р., а як P_1–P_n приймаємо середні ціни на акції компанії за аналогічний період, як P_b – середню ціну станом на 06.10.2009 р. Отже, біржові втрати становлять $504 М.

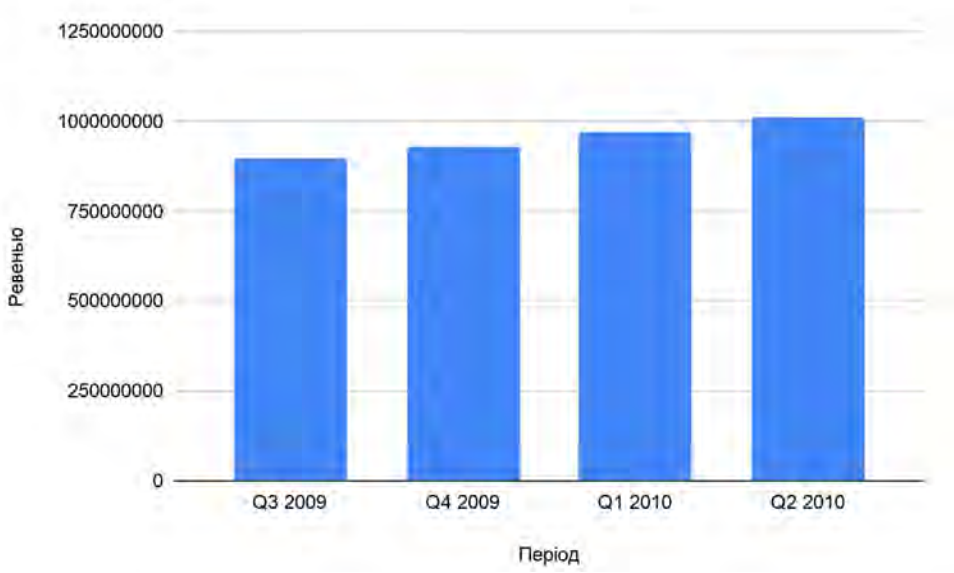

Рис. 6 Дані про ревенью компанії T-Mobile USA під час та після інциденту [16]

Аналіз показників прибутковості компанії в період інциденту, а також після нього (рис. 6) свідчить про відсутність помітного впливу на продажі. Зважаючи на це, а також не маючи інших точних даних про наслідки інциденту, можна зробити висновок, що в цьому випадку репутаційні втрати від інциденту дорівнюють біржовим втратам. Отже:

$$\sum_r = (\bar{P_b} - P_1)V_1 + \cdots + (P_b - P_n)V_n = \$504M,$$

де $\sum_r$ – сума економічних втрат, пов'язаних із репутаційними втратами; V_1–V_n – об'єми торгів акціями компанії, що зазнала репутаційних втрат впродовж розрахункового періоду; P_1–P_n – середні ціни на акції компанії, що зазнала репутаційних втрат впродовж розрахункового періоду; P_b – базова ціна на акції компанії, що зазнала репутаційних втрат до початку розрахункового періоду.

Отже, повні економічні втрати ($\sum_{\text{заг.}}$) від цього інциденту становлять:

$$\sum_{\text{заг.}} = \sum_i + \sum_r = \$107{,}9M + \$504M = \$601{,}9M.$$

Застосування помилкового алгоритму торгів високої швидкості. Компанія Knight Capital Group [6] була одним з лідерів маркет-мейкерів, що працювали на фондових біржах США. Основними видами діяльності компанії були прямий маркет-мейкінг та реалізація замовлень на виконання торговельних операцій із цінними паперами на біржі. Специфіка роботи фірми полягала у здійсненні так званих високошвидкісних торгів за допомогою програмного забезпечення, що виконує алгоритмічні дії на біржі. Програмне забезпечення знаходило пропозиції (бід та аск), що мають різницю (спред), та зверталось до продавця і покупця із пропозиціями, що дорівнювали їх пропозиціям. Отже, виконувалися обидві транзакції із набуванням комерційної вигоди. Вигода від однієї транзакції могла становити частки цента, але такі транзакції виконувалися до 40 разів за секунду.

1 серпня 2012 року Knight Capital планувала вийти на торги з оновленими алгоритмами. Торговельні сервери почали роботу нормально, але менш ніж за годину виявилось, що торги проходять в режимі, близькому до обвалу ринку, і роботу серверів Knight було зупинено. Робота

бірж одразу ж нормалізувалась. Невдовзі виявилося, що компанія втратила близько $460M доларів за 45 хвилин торгів [17].

Причини інциденту достеменно не відомі, адже компанія Knight Capital заявила лише про “певні проблеми” і точні причини відомого перебігу подій не розголошувала. Однак компанія Nanex, що займається моніторингом та аналізом біржових торгів, опублікувала детальний звіт про патерни, які демонстрували торговельні сервери Knight під час інциденту [18]. За словами аналітиків Nanex, система Knight Capital виходила із пропозицією про купівлю з найвищою ціною, що була на ринку, та із заявкою про продаж за найнижчою ціною. Розуміючи обсяги швидкісних торгів, легко зрозуміти, що втрата $460M за такого алгоритму цілком реальна. Пізніше Nanex опублікувала додатковий звіт із припущеннями, що на робочі сервери Knight Capital було помилково встановлено програмне забезпечення, яке діє як алготрейдер, але призначене для створення умов для тестування реальних алгоритмів швидкісної торгівлі на тестових біржах. Отже, сервери Knight Capital створювали вигідні позиції для алготрейдерів інших маркет-мейкерів. Така помилка є одним із негативних сценаріїв роботи систем безперервної інтеграції, що виконують завантаження і запуск нової версії. Логічно припустити, що в умовах реальної біржі алгоритми можуть працювати некоректно і завдавати збитків маркет-мейкеру або порушувати критерії “найкращого виконання” в разі опрацювання клієнтських заявок на продаж. Тож перевірка комерційної ефективності нового алгоритму на ранніх етапах його функціонування не допустила б настільки важких втрат. Звіт Nanex показує практичну можливість виявити такі відхилення швидко і з великою надійністю.

Компанія Knight Capital зазнала комплексних втрат і зрештою не змогла повністю відновитися. Через це наприкінці 2012 р. Knight поглинув конкурент GETCO за 1,4 мільярди доларів. Прямі збитки, як зазначено в звіті, становили 460 мільйонів доларів США, що можна розцінити як економічний результат від незворотних втрат [17].

Компанія Knight Capital не могла стабільно працювати без більшої частини оборотних коштів. Через це група інвесторів [19] терміново надала Knight Capital 400 мільйонів доларів США для відновлення капіталізації. Цю суму можна використовувати для економічного оцінювання супутніх витрат. Однак подія мала великий резонанс і спричинила глибоку кризу довіри з боку корпоративних клієнтів та інвесторів. Низка видань поширювала інформацію про масову відмову від послуг Knight з боку корпоративних клієнтів. Однак ґрунтовний аналіз фінансової звітності компанії за 2011–2012 рр. показав відсутність помітного впливу на цей напрям діяльності (рис. 7).

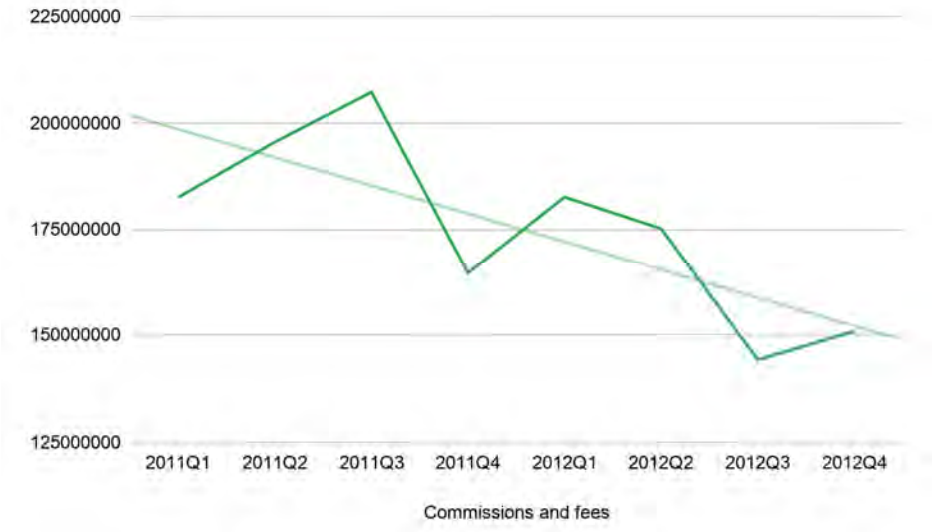

Рис. 7. Комісійні прибутки від виконання торговельних операцій клієнтів за 2011–2012 рр. [20]

Падіння у третьому кварталі 2012 р. не відрізняється істотно від загальної тенденції на спад, що спостерігалася протягом 2012 р. І більше, аналіз річної звітності показує поступове зниження

прибутків від розміщення заявок корпоративних клієнтів з 2009 р. [20]. Отже, немає достовірних факторів, що свідчили б про втрату вагомої частки ринку внаслідок інциденту.

Несуттєвість цих коливань добре видно порівняно із реакцією малих інвесторів, що спричинило катастрофічне падіння ціни на акції Knight[12]. Ціна цього асету зрештою так і не досягла тренду до відновлення навіть із урахуванням доінвестування.

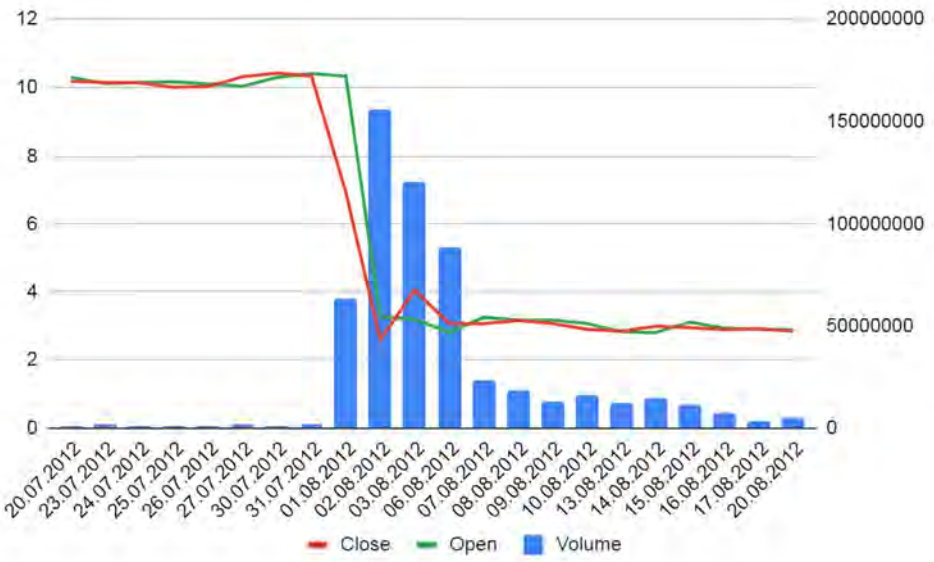

Рис. 8. Ціни асету KCG у період інциденту [12]

Зниження ціни на популярний асет спровокувало зростання обсягів торгів і, як наслідок, ще більшу паніку серед інвесторів та маркет-мейкерів. Розглянувши цей період детальніше, отримаємо графік, що містить дані для розрахунку економічних втрат.

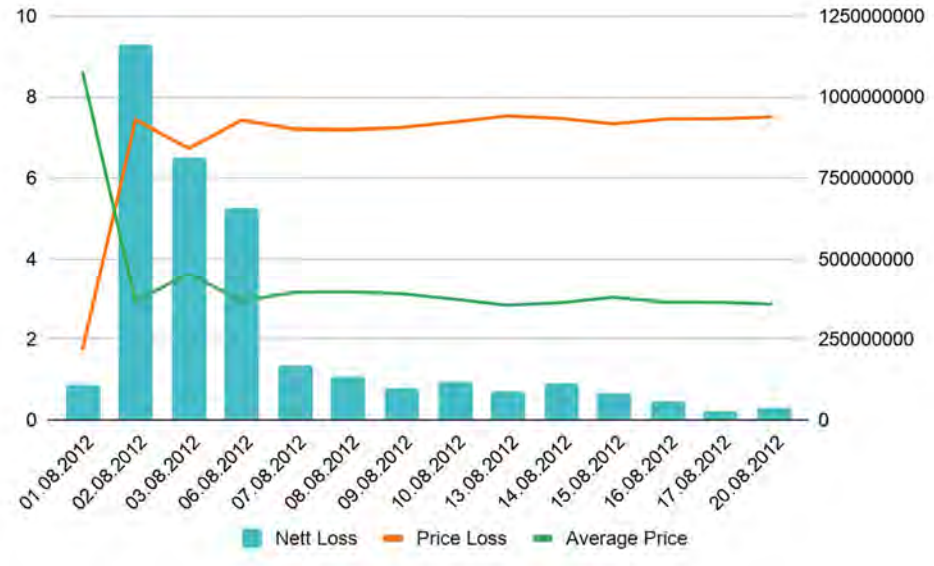

Рис. 9. Детальна динаміка здешевлення асету KCG після інциденту [12]

Використовуючи ці дані, розраховуємо загальний обсяг втрат від здешевлення акцій компанії. Як $V_1 - V_n$ приймаємо обсяги торгів акціями компанії, у період з 01.08.2012 р. до 20.08.2012 р., як

[12] NYSE: KCG

$P_1 - P_n$ – середні ціни на акції компанії за аналогічний період, як P_b – середню ціну станом на 30.07.2012 р. Отже, біржові втрати становлять $3663M. Враховуючи вищенаведену інформацію про відсутність достеменних ринкових втрат, вважаємо репутаційні втрати такими, що дорівнюють біржовим:

$$\sum_r = (P_b - P_1)V_1 + \cdots + (P_b - P_n)V_n = \$3663M,$$

де $\sum_r$ – сума економічних втрат, пов'язаних із репутаційними втратами; $V_1 - V_n$ – обсяги торгів акціями компанії, що зазнала репутаційних втрат впродовж розрахункового періоду; $P_1 - P_n$ – середні ціни на акції компанії, що зазнала репутаційних втрат впродовж розрахункового періоду; P_b – базова ціна на акції компанії, що зазнала репутаційних втрат до початку розрахункового періоду.

Отже, загальний економічний результат інциденту ($\sum_{\text{заг.}}$) можна подати як суму безпосередніх втрат унаслідок роботи помилкового алгоритму, доінвестування та репутаційних втрат:

$$\sum_{\text{заг.}} = \sum_i + \sum_r + \$460M + \$400M = \$4523M.$$

Висновки

Інциденти за участі компаній AECL, Raytheon та LAS показують, що ризик втрати людських життів може реалізуватися із настанням значних економічних втрат. Навіть якщо абстрагуватися від етичних питань, що постають під час розгляду цих випадків, їх економічний результат дає обґрунтовані підстави вважати, що сфера медичних послуг та оборонна сфера, а також будь-які сфери, що потенційно пов'язані із ризиком для людського життя, повинні приділяти велику увагу роботі із негативними сценаріями використання програмного забезпечення. Інцидент із LAS слід розглядати як показовий, оскільки ціла низка звітів та робіт із вивчення причин та наслідків [5], [13] вказує на ігнорування негативних сценаріїв використання системи її розробниками.

Наслідки втрати інформації через реалізацію негативних сценаріїв програмного забезпечення добре демонструє інцидент Sidekick. Потенційні витрати на задоволення групового позову, а також репутаційні збитки (падіння ціни на акції T-Mobile) вказують на вагомість економічних втрат, спричинених втратою даних. Цей тип втрат надзвичайно важливий для розроблення програмного забезпечення, оскільки дані завжди становлять об'єкт маніпуляції програмного забезпечення, тому завжди існує небезпека їх втрати. Отже, цінність таких даних можна за замовчуванням приймати як економічну вагу ризиків, пов'язаних із негативними сценаріями використання програмного продукту, що розглядається.

Перспективи подальших досліджень

Приклад Knight Capital Group показує можливий потенціал репутаційних втрат. Дуже важливо розуміти, що економічний результат від репутаційних втрат у цьому випадку більш ніж у дев'ять разів перевищив прямі збитки. Цю особливість також можна спостерігати на прикладі Sidekick (майже у п'ять разів). Цей факт змушує звернути увагу на надзвичайну актуальність цієї проблематики для публічних компаній. Варто звернути увагу на те, що економічні механізми виникнення таких значних економічних втрат полягають в ефектах роботи фондових бірж. Приклад Knight Capital Group також показує, що ці механізми можуть становити основу формування прямих збитків. Цей факт вказує на актуальність цієї проблематики для програмного забезпечення, що організує автоматизовану та автоматичну біржову діяльність.

Список літератури

1. Кузьмін О. Є. Економічне оцінювання та планування ризику нововведень на підприємствах машинобудування: монографія / О. Є. Кузьмін, Л. І. Чернобай, В. Ю. Харчук. Львів: Растр-7, 2011. 240 с.

2. The Monash University [https://www.monash.edu/]: THERAC-25 Computerized Radiation Therapy / Troy Gallagher. Режим доступу: https://web.archive.org/web/20071212183729/http://neptune.netcomp.monash.edu.au/cpe9001/assets/readings/www_uguelph_ca_~tgallagh_~tgallagh.html

3. University of Batch [https://www.bath.ac.uk/]: The Therac-25 Incident / Kimberley Chong. Режим доступ: http://people.bath.ac.uk/klzc20/CM50121cw1.pdf

4. University of Minnesota [https://twin-cities.umn.edu]: The Patriot Missile Failuret / Douglas N. Arnold. Режим доступу до публікації: http://www-users.math.umn.edu/~arnold//disasters/patriot.html

5. Darren Dalcher "Disaster in London. The LAS case study" Матеріали конференції Engineering of Computer-Based Systems, 1999. – Nashville, TN, USA, April 1999. Режим доступу: https://www.researchgate.net/publication/3792694_Disaster_in_London_The_LAS_case_study

6. Wikipedia, the free encyclopedia. Режим доступу: https://en.wikipedia.org

7. Маніна Л. І., Бондар-Підгурська О. В. Феномен "вартість життя людини" в контексті сталого соціально орієнтованого розвитку економіки // Матеріали Міжвузівського круглого столу, присвяченого Всесвітньому дню охорони праці. Полтава: Полтавський університет економіки і торгівлі, 28 квітня 2017 року. С. 66–67.

8. Canadian Coalition for Nuclear Responsibility [http://www.ccnr.org/]: Fatal Dose. Radiation Deaths linked to AECL Computer Errors / Barbara Wade Rose // Опубліковано 1994 р. Режим доступу: http://www.ccnr.org/fatal_dose.html

9. Canadian Coalition for Nuclear Responsibility [http://www.ccnr.org/]: The Economic Costs of the Canadian Nuclear Industry / David Martin and David Argue // Опубліковано 1996 р. Режим доступу: http://www.ccnr.org/sunset_table.html#E&Y

10. Report to the Chairman, Subcommittee on Investigations and Oversight, Committee on Science, Space, and Technology, House of Representatives / PATRIOT MISSILE DEFENSE. Software Problem Led to System Failure at Dhahran, Saudi Arabia / Washington, D. C.: United States General Accounting Office, 1992. 18 с.

11. Електронне видання "Military.com" [https://www.military.com]: Death Gratuity / автора допису не зазначено // Опубліковано 2019 р. Режим доступу: https://www.military.com/benefits/survivor-benefits/death-gratuity.html

12. Yahoo Finance / Публічна база даних фінансової інформації. Режим доступу: https://finance.yahoo.com

13. Report of the Inquiry Into The London Ambulance Service [Текст] / South West Thames Regional Health Authority: London, United Kingdom. Режим доступу: http://www0.cs.ucl.ac.uk/staff/A.Finkelstein/las/lascase0.9.pdf

14. The Secretary of State for Health Report to the Parliament of the United Kingdom [Текст] / Virginia Bottomley / London, United Kingdom. Режим доступу: https://publications.parliament.uk/pa/cm199293/cmhansrd/1992-10-28/Debate-1.html

15. Class Action / Northern District of California United States District Court / Maureen Thompson, an individual, on behalf of herself and all others similarly situated v. T-MOBILE USA, INC., DANGER, INC., and MICROSOFT CORPORATION [Текст]: San Francisco, USA, 2009. Режим доступу: https://web.archive.org/web/20091024183301/http://www.prnewschannel.com/pdf/10-14-09_Complaint_SideKick.pdf

16. Macrotrends / Публічна база даних фінансової інформації. Режим доступу: www.macrotrends.net

17. Report In the Matter of Knight Capital Americas LLC Respondent, File No. 3-15570 [Текст] / U. S. Securities and Exchange Commission: Washington, D. C., USA. Режим доступу: https://www.sec.gov/litigation/admin/2013/34-70694.pdf

18. Report "01-Aug-2012 ~ Knightmare on Wall Street" [Текст] / Nanex, LLC: Winnetka, Illinois, USA. Режим доступу: http://www.nanex.net/aqck2/3522.html

19. The Reuters [https://www.reuters.com]: Knight Capital posts $389.9 million loss on trading glitch / John McCrank // Опубліковано 2012 р. Режим доступу: https://www.reuters.com/article/us-knightcapital-results/knight-capital-posts-389-9-million-loss-on-trading-glitch-idUSBRE89G0HI20121017

20. SEC Report / Публічна база даних фінансової інформації Комісії з цінних паперів та бірж США. Режим доступу: https://sec.report/

Reference

1. Kuzmin O. (2011). Ekonomichne otsinyuvannya ta planuvannya ryzyku novovveden na pidpryyemstvakh mashynobuduvannya: monohrafiya [Economic evaluation and risk planning of innovations at machine-building enterprises: monograph], Lviv, Raster-7 Publishing House, 240 p.

2. Troy Gallagher THERAC-25 Computerized Radiation Therapy. The Monash University. Retrieved from: https://web.archive.org/web/20071212183729/http://neptune.netcomp.monash.edu.au/cpe9001/assets/readings/www_uguelph_ca_~tgallagh_~tgallagh.html

3. Kimberley Chong The Therac-25 Incident University of Batch. Retrieved from: http://people.bath.ac.uk/klzc20/CM50121cw1.pdf

4. Douglas N. Arnold The Patriot Missile Failuret. University of Minnesota. Retrieved from: http://www-users.math.umn.edu/~arnold//disasters/patriot.html

5. Darren Dalcher (1999). "Disaster in London. The LAS case study": Engineering of Computer-Based Systems, – Nashville, TN, USA, April 1999. Retrieved from: https://www.researchgate.net/publication/3792694_Disaster_in_London_The_LAS_case_study

6. Wikipedia, the free encyclopedia. Retrieved from: https://en.wikipedia.org

7. Manina L., Bondar-Pidhurs'ka O. (2017). Fenomen "vartist zhyttya lyudyny" v konteksti staloho sotsialno oriyentovanoho rozvytku ekonomiky ["Phenomenon of life value" in the context of sustainable socially oriented economic development.]. Retrieved from http://194.44.39.210/bitstream/123456789/6354/1/%D0%9A%D1%80%D1%83%D0%B3%D0%BB%D0%B8%D0%B9%20%D1%81%D1%82%D1%96%D0%BB%202017%207.pdf

8. Barbara Wade Rose (1994) Fatal Dose. Radiation Deaths linked to AECL Computer Errors. Canadian Coalition for Nuclear Responsibility, Retrieved from: http://www.ccnr.org/fatal_dose.html

9. David Martin, David Argue (1996) The Economic Costs of the Canadian Nuclear Industry. Canadian Coalition for Nuclear Responsibility. Retrieved from: http://www.ccnr.org/sunset_table.html#E&Y

10. Report to the Chairman, Subcommittee on Investigations and Oversight, Committee on Science, Space, and Technology, House of Representatives / PATRIOT MISSILE DEFENSE. Software Problem Led to System Failure at Dhahran, Saudi Arabia / Washington, D.C.: United States General Accounting Office, 1992.

11. Military.com (2019). Death Gratuity. Retrieved from: https://www.military.com/benefits/survivor-benefits/death-gratuity.html

12. Yahoo Finance. Retrieved from: https://finance.yahoo.com

13. Report of the Inquiry Into The London Ambulance Service / South West Thames Regional Health Authority: London, United Kingdom. Retrieved from: http://www0.cs.ucl.ac.uk/staff/A.Finkelstein/las/lascase0.9.pdf

14. The Secretary of State for Health Report to the Parliament of the United Kingdom / Virginia Bottomley / London, United Kingdom. Retrieved from: https://publications.parliament.uk/pa/cm199293/cmhansrd/1992-10-28/Debate-1.html

15. Class Action / Northern District of California United States District Court / Maureen Thompson, an individual, on behalf of herself and all others similarly situated v. T-MOBILE USA, INC., DANGER, INC., and MICROSOFT CORPORATION: San Francisco, USA, 2009. Retrieved from: https://web.archive.org/web/20091024183301/http://www.prnewschannel.com/pdf/10-14-09_Complaint_SideKick.pdf

16. Macrotrends. Retrieved from: www.macrotrends.net

17. Report In the Matter of Knight Capital Americas LLC Respondent, File No. 3-15570 U. S. Securities and Exchange Commission: Washington, D.C., USA. Retrieved from: https://www.sec.gov/litigation/admin/2013/34-70694.pdf

18. Report "01-Aug-2012 ~ Knightmare on Wall Street" Nanex, LLC: Winnetka, Illinois, USA. Retrieved from: http://www.nanex.net/aqck2/3522.html

19. John McCrank (2012) Knight Capital posts $389.9 million loss on trading glitch. The Reuters. Retrieved from: https://www.reuters.com/article/us-knightcapital-results/knight-capital-posts-389-9-million-loss-on-trading-glitch-idUSBRE89G0HI20121017

20. SEC Report. Retrieved from: https://sec.report/

O. Ye. Kuzmin, N. S. Stanasyuk, D. A. Berdnik
Lviv Polytechnic National University

EXAMPLES OF EXPENSES RELATED TO NEGATIVE SCENARIOS OF SOFTWARE USE

This paper represents a list of widely known issues of risk implementation related to specific negative scenarios of software use. The core selection criteria were an opportunity to identify impact areas that led to the core losses for each case. Main preconditions, course of events and consequences are highlighted. In addition, it is explicitly defined which negative scenario was ignored or missed and how it led to the damage.

This article is aside from the classical definition of "bug", but focusing on negative use cases (negative scenarios) ignored or mistreated during requirement engineering, development, and testing. By stating a bug modern software development usually, means a mistake in source code or misalignment of settings between program components. Meanwhile, a negative scenario means something able to be performed using normally operating software. Negative scenario is something average user typically not do. However, basing on experience or logic analysis we can assume negative scenarios able to appear, list them, evaluate possible consequences and enhance the software in a manner preventing scenario execution or consequences. As the study shows, that all listed negative scenarios are typical from the general software development or domain point of view. So all listed consequences were able to be mitigated or avoided at all.

All these issues are equipped with a numerical value of economical losses defined based on studies' data or reports given by different authorities in regards to these cases. All cases belong to different domains, it helps to highlight areas of modern business able to cause similar losses in case if negative scenarios take place.

All this data proves the necessity of negative scenarios mitigation during software development. The given examples explicitly show that high impact may take place in various domains. What makes negative use cases a common problem for a variety of applications in the international and domestic economy. However, in some cases possible impact may appear not explicitly and obviously enough. From such a perspective, it is very important to collect, classify and evaluate cases related to negative use cases implementation to provide information important for further development.

The study shows the referring field for risk managers, project managers and all risk assessment professionals. It provides examples of negative software use cases appearing and causing damage in an area this software is used in. This referring field should help software development specialists to take a proper decision regarding negative scenarios risks arising. Also, this paper emphasizes the extremely powerful impact of negative scenarios on software related to exchanges, which creates an additional area for perspective research.

Key words: negative scenario; economic effect; losses; software development.