УДК 338.054.23

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

ПРИКЛАДИ РЕЗУЛЬТАТІВ ВІД ДІЇ НЕГАТИВНИХ СЦЕНАРІЇВ ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

http://doi.org/

Представлено приклади широко відомих випадків настання ризиків, пов'язаних із негативними сценаріями використання програмного забезпечення, що принесли вагомі втрати власникам, авторам чи суспільству. Основним критерієм для пошуку та вибору таких прикладів стала достовірність, вагомість та можливість навести точні дані про економічні втрати або порядок втрат. Висвітлені 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

В якості інструмента описання роботи програмного забезпечення використовується написання позитивних сценаріїв використання додатків, так званих "історій користувачів". Під позитивним сценарієм розуміється певна послідовність дій користувача, що неодмінно приводить до виконання бізнес-функції додатку та досягнення бізнес-цілі, що ставиться на меті 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, що він має виконати з допомогою додатку, що описується. За допомогою множини позитивних сценаріїв повністю описується бізнес-мета програмного забезпечення з ціллю його подальшого розроблення.

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

В низці випадків практичну користь у процесі прийняття рішень може нести приклад випадку, що мав місце в аналогічній галузі або в процесі використання аналогічного програмного забезпечення. Такі приклади дають розуміння наявності областей сучасного бізнесу, що пов'язані із значним ризиком вагомих втрат. Більше того, в деяких випадках є можливість знайти приклади, що описують не тільки аналогічну сферу, а й аналогічні бізнес-цілі додатку.

[1] Client Relationship Management systems

Актуальність дослідження

Важливим аспектом сучасного планування проектних робіт є формування множини негативних сценаріїв, що необхідно врахувати. Як правило, для прийняття рішення щодо необхідності блокування того чи іншого негативного сценарію враховується оцінка можливих економічних наслідків, його реалізації та вірогідність настання такого сценарію або порівняння із втратами, що мали місце при розробленні аналогічних додатків чи додатків в аналогічній сфері. Таким чином, однією з цілей сучасного розроблення програмного забезпечення є блокування виконання негативних сценаріїв, чи попередження про можливі наслідки. Така ціль досягається з допомогою двох основних етапів. По-перше, при розробленні технічної документації до проекту обробляються типові або специфічні для області застосування негативні сценарії із метою виявлення критичних ризиків та розроблення елементів програмного забезпечення, що блокує виконання таких сценаріїв. По-друге, під час перевірки якості програмного забезпечення перевіряються і негативні сценарії.

Формулювання мети та завдань статті

Основна мета даної роботи – обґрунтувати необхідність врахування негативних сценаріїв використання програмного забезпечення підчас його розроблення; надати спеціалістам із управління ризиками, менеджерам проектів 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 із допомогою історичних аналогів.

Аналіз останніх досліджень і публікацій

Зазначимо, що загальний підхід до розгляду ризиків підчас впровадження нововведень розглянуто у роботі [1]. Крім того, ряд вчених розглядає конкретні випадки втрат від певних негативних сценаріїв використання програмного забезпечення, фокусуючись на деталях та перебігу подій в рамках одного інциденту. Такі роботи надають повну інформацію про певну подію, а також оцінку автора по відношенню до 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 в роботі Darren Dalcher[5], що ретельно дослідив колапс Лондонської системи невідкладної допомоги. В контексті зазначеного виникає необхідність Однак, роботи, в якій би проводилося порівняння низки інцидентів в контексті впливу негативних сценаріїв використання програмного забезпечення знайти не вдалося.

Виклад основного матеріалу

Для розгляду дії негативних сценаріїв використання програмного забезпечення на базі прикладів, що мали місце в різних сферах сучасного бізнесу розглянемо ряд випадків. Їх економічний результат буде розглянуто за наступними класами втрат (якщо такі мали місце): незворотні втрати, втрати інформації, втрати операційного часу, репутаційні втрати. Для кожного випадку буде підрахований повний економічний результат.

Некоректна робота апарату Therac 25. Даний апарат був розроблений підрозділом[2] канадської державної компанії Atomic Energy of Canada Limited (далі AECL) у 1982 році як продовження успішної моделі Therac 20 і використовувався для комплексної променевої терапії [6]. Як виявилось згодом, упродовж 1985 – 1987 років специфічний сценарій використання цього апарату спричинив щонайменше 6 випадків важкої променевої хвороби у пацієнтів, що отримували променеву терапію [2]. Достеменно відомо, що двоє з них загинуло саме від наслідків променевої

[2] В якості окремої організації відомий як "Radiochemical Company"

хвороби. Вага негативного впливу апарату Therac 25, в якості основної причини смерті інших постраждалих може ставитися під сумнів з огляду на їх стан на момент початку терапії.

Цей випадок є показовим з ряду причин. По-перше, з усієї серії апаратів Therac саме Therac 25 вперше мав тільки електроний, а не механічний захист від надмірного опромінення. Тобто ми говоримо про значний інцидент з точки зору зони відповідальності програмного забезпечення. По-друге, аналіз причин виникнення передумов інцидентів вказує на організаційні недоліки, що передусім призводили до відсутності уваги до негативних сценаріїв, інтеграційних сценаріїв апаратної та програмної складової, а також до загального низького рівня перевірки як сценаріїв використання програмного продукту, так і апарату в цілому. Не зважаючи на ризикований та амбітний крок по відмові від механічного контролю за радіаційною безпекою, що мав би ініціювати розроблення нового програмного забезпечення, для Therac 25 використовувалася модифікована програмна компонента апарату Therac 20, який мав механічний захист. Саме наявність механічного захисту від надмірного опромінення блокувало альтернативний сценарій, що став причиною інцидентів.

Оцінюючи економічні наслідки слід звернути увагу саме на людські жертви, оскільки фінансові втрати компанії були частково або повністю покриті страховками і наявність позовів з боку жертв або їх родичів по всіх випадках сумнівна[3]. Таким чином до уваги може бути взята лише еквівалентна 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, що мала місце заборона на використання продуктів компанії з 1991 по 1994[8] рік. Хоча вона була повною лише впродовж 1991 року, і аж до повної відміни носила частковий характер. Точні економічні показники від втрати операційного часу встановити важко адже немає точних даних про недоотриманий прибуток.

Економічний результат від репутаційних втрат можна відстежити, аналізуючи подальший розвиток підрозділу Radiochemical Company. Даний підрозділ було продано в якості окремої компанії у 1988 році[9]. Передусім треба розуміти, що поспіх із яким підрозділ було приватизовано та продано[3] приватним інвесторам, свідчить про те, що компанія AECL, що передусім спеціалізується не устаткування для атомної енергетики, прагнула зменшити репутаційний вплив на свій основний бізнес. Однак за фактом цієї угоди канадському уряду довелося зробити декілька компенсацій[9]:

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

Також сюди слід додати знижку в $14,5M, яку було надано під час продажу. Компанія AECL безперечно зіткнулася з значними ринковими наслідками репутаційних втрат і зниженням довіри до власних продуктів. Точний економічний результат встановити важко, оскільки а ні компанія AECL, а ні її підрозділ не публікували публічних звітів на час інциденту. Однак достеменно відомо про повернення принаймні 6 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.

[3] Під назвою Nordion International Inc.

[4] Середня ціна подібного апарату становить приблизно $3M.

Таким чином, 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 Персидській Затоці для оборони ряду військових об'єктів коаліції[6] та мирних жителів на території Саудівської Аравії було розгорнуто батарею зенітно ракетних комплексів (ЗРК) Патриот[5]. Комплекси мали здійснювати перехоплення ракет класу земля-земля, випущених військами Іраку. Характеристики ЗРК, а також диспозиція дозволяли перехопити всі можливі цілі, що могли бути використані противником. Однак, 25 лютого 1991 року ракета SCUD[6] влучила у барак із військовослужбовцями армії США. Внаслідок прямого попадання загинуло 28 бійців та близько 100 дістали поранення. Ракета Патріот, що була 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 було здійснено через похибку у розрахунку часу підльоту ракети супротивника. Програма управління комплексом містила методи, що визначали час у долях секунди із похибкою. Дана похибка була незначна і при стандартних випробуваннях не давалася взнаки, але при безперервній роботі впродовж більш як 20 годин – створювала помилку наведення більшу за зону контакту (фактичний проліт повз). На момент інциденту комплекси знаходилися на бойовому чергуванні орієнтовно 100 годин. Основною причиною цієї проблеми було те, що сама по собі похибка була замалою для того, щоб мати значущий вплив (та бути виявленною підчас випробувань), але вона мала акумулятивний ефект, який можна було виявити лише підчас довгострокових випробувань. Нестандартний час роботи є одним з типових негативних сценаріїв використання програмного забезпечення і наразі широко використовується для моделювання роботи важливих систем.

Розглядаючи наслідки трагедії варто звернути увагу на кількість жертв, що є над великою навіть із огляду на стан війни. Згідно із законодавством США загибель або отримання каліцтв військовослужбовцями 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 об'єм виплат пораненим встановити важко, оскільки відсутні публічні дані про ступінь поранень та втрату працездатності через них.

Втрати від знищення військового майна не розголошуються. Однак у доступних джерелах згадується про знищення бараку (більш значні об'єкти військового майна не згадуються).

Таким чином, незворотні втрати можна вирахувати 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 даних комплексів, але, на жаль, з огляду на об'єктивні причини неможливо відслідкувати динаміку подальших продажів чи долю ринку. Але історія цін на акції компанії Raytheon[7], що є виробником комплексу, доступна у публічних джерелах[12].

Аналіз історії біржових торгів по даному асету показав, що у період інциденту (рис. 1), а також у період публікації звіту (рис. 2) визначних трендових падінь не відбувалося. Отже, встановлено відсутній або наявність незначного впливу інциденту на загальні показники компанії виробника.

[5] Зенітноракетний комплекс MIM-104 Patriot

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

[7] NYSE: RTN

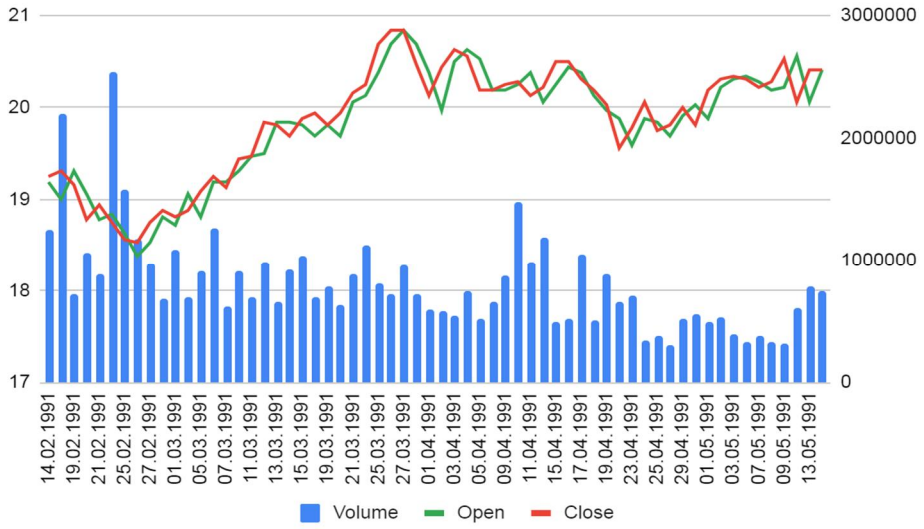

Рис. 1. Ціни асету RTN[12] впродовж трьох місяців від інциденту

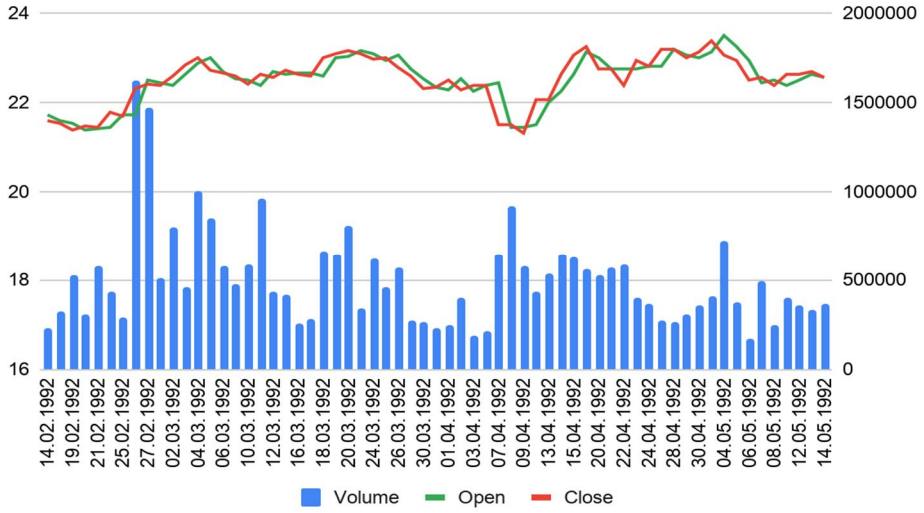

Рис. 2. Ціни асету RTN[12] впродовж трьох місяців від публікації звіту[10]

Оскільки неможливо встановити чи мала місце втрата цінних даних, а також втрата операційного часу, економічний результат (від інциденту (той що можна обчислити за наявних даних) дорівнює економічному результату від незворотних втрат, а саме:

.

Колапс системи розподілення карет швидкої допомоги міста Лондон є одним з найпоказовіших з огляду на масштаб, кількість проблем і широкий огляд у пресі, офіційних звітах[13] та наукових роботах з управління ризиками, якістю та проектами. 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 роботи над помилками, причиною інциденту стали значні помилки в організації проекту, низька якість наданого програмного забезпечення, а також помилки в управлінні вимогами. З вище наведених причин варто звернути увагу на те, що всі без винятку робітники служби швидкої допомоги (від операторів колл центрів до медичного персоналу швидких) не приймали участі у формуванні вимог до програмного комплексу,

а також його прийомі. Таким чином, реальний практичний досвід не брався до уваги як такий. Брався до уваги лише ідеальний перебіг подій без детального розуміння його етапів.

Для предмету даної статті інтерес становлять саме негативні сценарії використання програмного забезпечення, що через помилки в управлінні вимогами не були враховані та становили значний негативний вплив на перебіг подій. Більшість авторів, що проводили аналіз даного інциденту наводять наступні негативні сценарії, що мали вирішальний вплив:

1. Система не могла обробляти заявки на надання невідкладної допомоги, що не містили повної інформації про постраждалого, інцидент та багато іншого. Такий недолік спричинив значну затримку в оформленні звернень, а також значну кількість даних, що не відповідали дійсності і були введені лише для того, щоб система прийняла заявку.
2. Система не могла виявляти та обробляти дублі, тому повторні виклики від людей, що не дочекалися швидкої, додавалися до списку активних викликів і до однієї і тої самої адреси направляли декілька карет.
3. В 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 відключити системні повідомлення). Через це за кілька годин термінали в каретах швидкої були фактично заблоковані і медичний персонал не мав змоги прийняти виклик.
5. Система не могла обробити неточну інформацію від модулів визначення положення швидких. З цієї причини екіпажі, що на момент створення виклику рухалися або їх модуль був під впливом радіо-перешкод (що досить типово у великому місті) ігнорувалися і виклик передавався 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 людських жертв. Використовуючи показники, запропоновані у роботі[7] отримано наступний 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 несли відповідальність за надання невідкладної допомоги, так і на приватні компанії, що мали відношення 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 проекту 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 припинила своє існування через репутаційні втрати. Значних репутаційних втрат зазнала і LAS, що призвело до значних 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 році. Беручи до уваги опубліковані чисельні показники, загальний результат від інциденту ($\sum_{заг.}$) можна представити 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, що була розроблена компанією Danger та пропонувалася спільно із телекомунікаційною компанією T-Mobile USA на

[8] За курсом 1992 року це становить приблизно $2650000

ринку Сполучених Штатів Америки. Орієнтовно в період з 29 вересня до 6 жовтня 2009 року компанія втратила особисті дані більш як 800 000 клієнтів[6].

Однією з головних переваг цього пристрою була регулярна процедура копіювання даних користувача (адресна книга, дописи, фото, повідомлення, розклад, тощо) на сервера 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 має вплив на репутацію хмарних сервісів та довіру до них. По-третє, оскільки компанія Danger у 2008 році була поглинута компанією Microsoft, і на час інциденту являла собою структурний підрозділ компанії, даний випадок став одним з чинників негативного суспільного ставлення до аквізицій з боку Microsoft.

Програмне забезпечення, що контролює систему бекапів Sidekick ігнорувала досить вірогідний негативний сценарій, а саме втрата копії даних на хмарному сервері. В разі виходу із строю сервера або втрати зв'язку із ним дані, що знаходилися на пристрої вважалися недостовірними за замовчуванням. Більш того, при перезавантаженні пристрою дані на ньому видалялися автоматично, оскільки вважалися неактуальними, і мали бути завантаженими з сервера. Також не було можливості скопіювати наявну на пристрої інформацію на інший носій або компьютер. Отже після технічних проблем із серверним устаткуванням пристрої, що перезавантажувалися, видаляли всю наявну на пристрої інформацію.

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

Ключовим для розуміння збитків від втрати даних є груповий позов, який мав місце по відношенню до компанії T-Mobile USA [15]. Ще до розгляду справи компанія надіслала постраждалим користувачам подарункові карти номіналом $100, що можна було використати для оплати послуг T-Mobile. Після розгляду справи було присуджено додаткову виплату (у формі послуг та контенту) в розмірі $34,88. Таким чином, 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.

Акції компанії Microsoft[9] не зазнали помітного ефекту від подій, що описуються або публікації рішень суду (рис. 3). Така відсутність реакції може пояснюватися тим, що Danger, або Microsoft Azure[10] не мають окремого біржового індексу, тож MSFT показує загальний інтерес до компанії та її продуктів, включаючи як проблемні активи, так і успішні.

В той самий час акції компанії T-Mobile[11] зазнали довгострокового тренду на здешевлення, що однозначно показує важкий вплив на репутацію компанії (рис. 4).

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

Використовуючи ці дані розраховуємо загальний об'єм втрат від здешевлення акцій компанії (витрати, які необхідно здійснити для відновлення початкової ціни асету). В якості $V_1 - V_n$ приймаємо об'єми торгів акціями компанії, у період з 07.10.2009 по 11.11.2009, в якості $P_1 - P_n$ приймаємо середні ціни на акції компанії за аналогічний період, в якості P_b – середню ціну станом на 06.10.2009. Таким чином, біржові втрати становлять $504M.

[9] NasdaqGS: MSFT

[10] Хмарний сервіс від компанії Microsoft

[11] NasdaqGS: TMUS

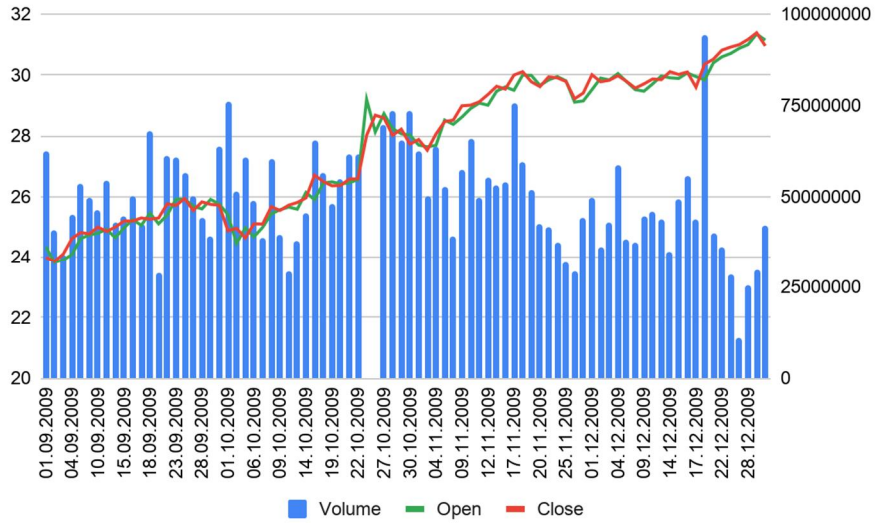

Рис. 3 Ціни асету MSFT від початку інциденту [12]

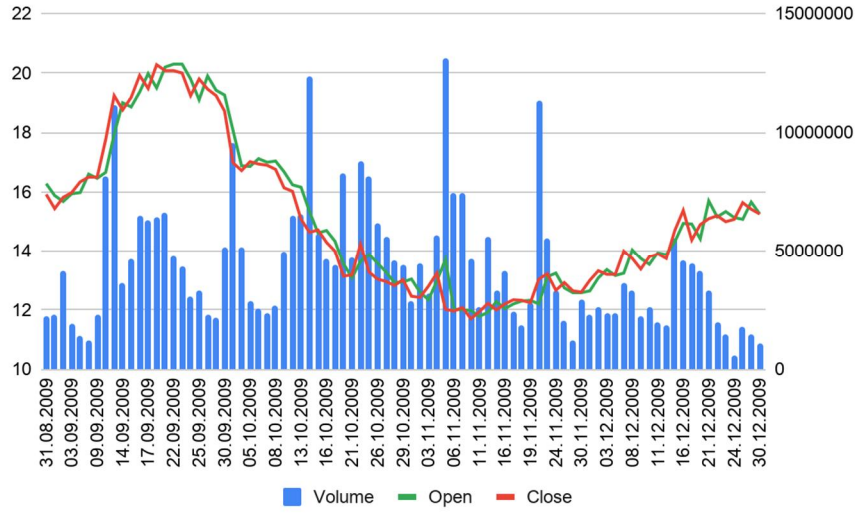

Рис. 4 Ціни асету TMUS на момент інциденту та після нього[12]

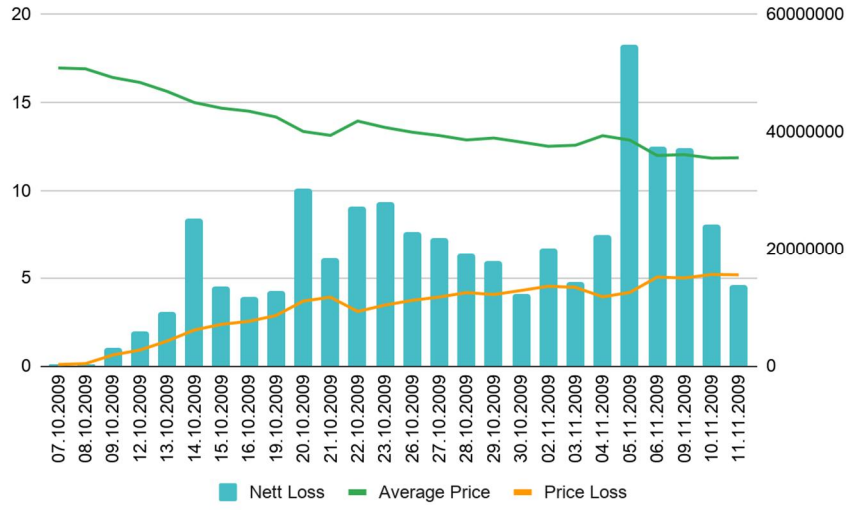

Рис. 5 Детальна динаміка здешевлення асету TMUS після інциденту [12]

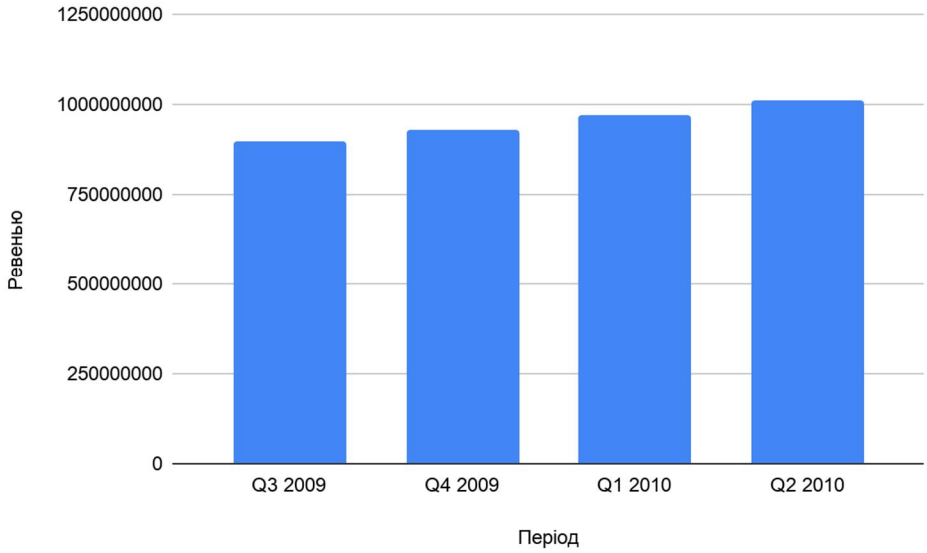

Рис. 6 Дані про ревенью компанії T-Mobile USA підчас та після інциденту [16]

Аналіз показників прибутковості компанії в період інциденту, а також після нього (рис. 6), показує відсутність помітного впливу на продажі. Виходячи з цього, а також не маючи інших точних даних про наслідки інциденту можна зробити висновок, що в даному випадку репутаційні втрати від інциденту дорівнюють біржовим втратам. Таким чином:

,

де – сума економічних втрат, пов'язаних із репутаційними втратами, – об'єми торгів акціями компанії, що понесла репутаційні втрати впродовж розрахункового періоду, – середні ціни на акції компанії, що понесла репутаційні втрати впродовж розрахункового періоду, – базова ціна на акції компанії, що понесла репутаційні втрати до початку розрахункового періоду.

Отже, повні економічні втрати (від даного інциденту становлять:

.

Застосування помилкового алгоритму торгів високої швидкості. Компанія Knight Capital Group[6] була одним з лідируючих маркет-мейкерів, що працювали на фондових біржах США. Основними видами діяльності компанії були прямий маркет-мейкінг та реалізація замовлень на виконання торгових операцій із цінними паперами на біржі. Специфіка роботи фірми полягала у виконанні 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 виходило до продавця і покупця із пропозиціями, що дорівнювали їх пропозиціям. Таким чином, виконувалися обидві транзакції із набуванням комерційної вигоди. Вигода від однієї транзакції могла складати долі центу, але подібні транзакції виконувалися до 40 разів на секунду.

1 серпня 2012 року Knight Capital мала вийти на торги з оновленими алгоритмами. Торгові сервери почали роботу нормально, але менш, ніж за годину було виявлено, 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 розголошувалися. Однак, компанія Nanex, що займається моніторингом та аналізом біржових торгів опублікувала детальний звіт про

патерни, що демонстрували торгівельні сервери Knight підчас інциденту[18]. За словами аналітиків Nanex, система Knight Capital виходила з пропозицією про купівлю з найвищою ціною, що наявна на ринку, та з заявкою про продаж за найнижчою ціною. Розуміючи об'єми швидкісних торгів, можна 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, що діє як алготрейдер, але призначене для створення умов для тестування реальних алгоритмів швидкісної торгівлі на тестових біржах. Таким чином сервери Knight Capital створювали вигідні позиції для алготрейдерів інших маркет мейкерів. Подібна помилка є одним з 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 збитки 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 подібні відхилення в короткий термін і з великою надійністю.

Компанія Knight Capital зазнала комплексних втрат і з рештою не змогла повністю відновитися. Через це наприкінці 2012 року відбулося поглинення Knight конкурентом GETCO за 1,4 мільярди доларів. Прямі збитки, як зазначається в репорті склали 460 мільйонів доларів США, що можна розцінити як економічний результат від незворотних втрат [17].

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

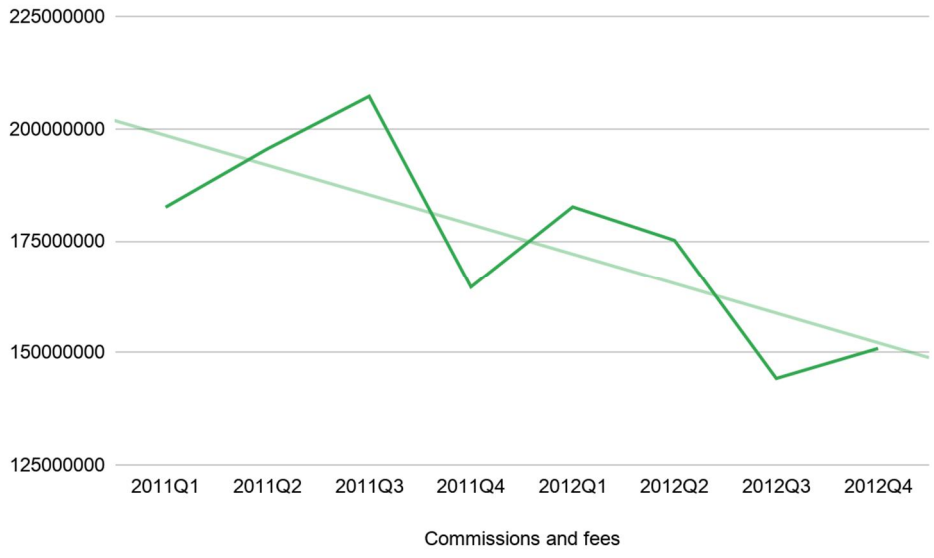

Рис. 7 Комісійні прибутки від виконання торговельних операцій клієнтів за 2011 – 2012 роки[20]

Падіння у третьому кварталі 2012 року не відрізняється суттєво від загальної тенденції на спад, що спостерігається протягом 2012 року. Більш того, аналіз річної звітності показує поступове зниження прибутків від розміщення заявок корпоративних клієнтів починаючи з 2009 року [20].

Таким чином, немає достовірних факторів, що б свідчили про втрату вагомої долі ринку внаслідок інциденту.

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

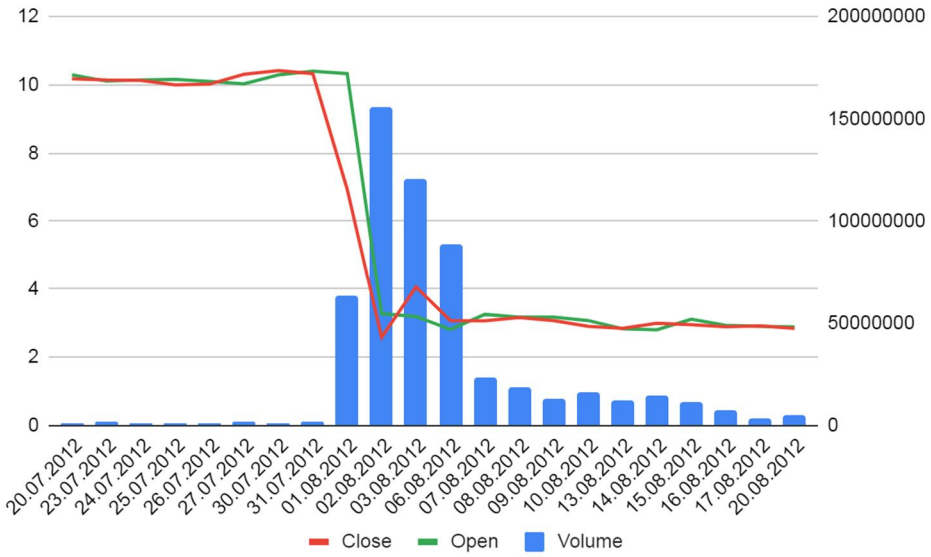

Рис. 8 Ціни асету KCG в період інциденту [12]

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

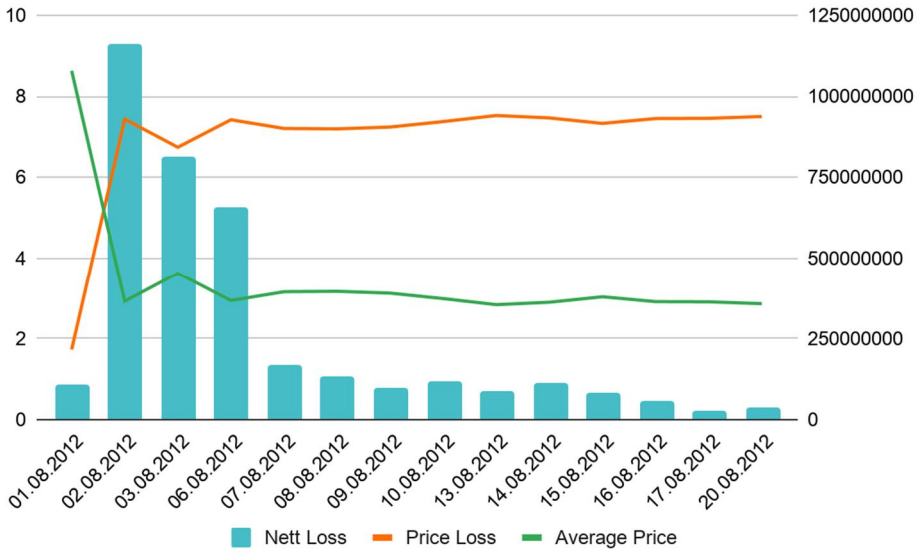

Рис. 9 Детальна динаміка здешевлення асету KCG після інциденту[12]

Використовуючи ці дані розраховуємо загальний об'єм втрат від здешевлення акцій компанії. В якості приймаємо об'єми торгів акціями компанії, у період з 01.08.2012 по 20.08.2012, в якості приймаємо середні ціни на акції компанії за аналогічний період, в якості –

[12] NYSE: KCG

середню ціну станом на 30.07.2012. Таким чином, 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, $V_1 - V_n$ – об'єми торгів акціями компанії, що понесла репутаційні втрати впродовж розрахункового періоду, $P_1 - P_n$ – середні ціни на акції компанії, що понесла репутаційні втрати впродовж розрахункового періоду, P_b – базова ціна на акції компанії, що понесла репутаційні втрати до початку розрахункового періоду.

Таким чином загальний економічний результат інциденту ($\sum_{\text{заг.}}$) можна представити, як суму безпосередніх втрат від 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 при розгляді цих випадків, їх економічний результат дає чіткі підстави вважати, що сфера медичних послуг та оборонна сфера, а також будь які сфери, що потенційно пов'язані з ризиком для людського життя, мають приділяти велику увагу роботі із негативними сценаріями використання програмного забезпечення. Інцидент з LAS слід розглядати як показовий, оскільки цілий ряд звітів та робіт з 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 показує 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 є небезпека втрати цих даних. 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 важливим є розуміння факту, що економічний результат від репутаційних втрат в цьому випадку більш як в 9 разів перевищив прямі збитки. Цю особливість також можна спостерігати у прикладі Sidekick (майже в 5 разів). Цей факт змушує звернути увагу на надзвичайну актуальність даної 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 даної 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: Видавництво "Растр-7», 2011. – 240 с.

2. The Monash University [https://www.monash.edu/] : THERAC-25 Computerized Radiation Therapy / Troy Gallagher – Режим доступу до публікації. : 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 доступу до публікації: 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 до публікації: https://www.researchgate.net/publication/3792694_Disaster_in_London_The_LAS_case_study

6. Wikipedia, the free encyclopedia – Режим доступу до ресурсу : 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 до публікації. : 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 до публікації. : 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 / автор допису не зазначений // Опубліковано 2019 р. – Режим доступу до публікації. : https://www.military.com/benefits/survivor-benefits/death-gratuity.html

12. Yahoo Finance / Публічна база даних фінансової інформації – Режим доступу до ресурсу: 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 до звіту: 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 до звіту: 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 до публікації: 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 до ресурсу: 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 до звіту: 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 до звіту: 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 до публікації. : 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 до ресурсу: https://sec.report/

Reference

1. O. Kuzmin (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" Матеріали конференції 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. L. Manina, O. Bondar-Pidhurs□ka (2017) *Fenomen "vartist□ zhyttya lyudyny" v konteksti staloho sotsial□no 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. – 18 c.

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. Kuzmin, N. Stanasyuk, D. 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.