УДК 004.94

Шевченко А. В., (ORCID 0000-0003-3793-9364)

Державний університет телекомунікацій, Київ

Управління функціональною стійкістю інформаційних систем на основі оптимізації видатків на захист

Резюме. Проаналізовано стан, напрями та основні причини зростання кількості інцидентів інформаційної безпеки. Побудовано моделі залежності збитків від інцидентів, як функцій від видатків на інформаційну безпеку. Знайдено загальну залежність оптимальних видатків на інформаційну безпеку залежно від рівня критичності інформаційних ресурсів організації.

Ключові слова: інциденти; інформаційна безпека; функціональна стійкість; інформаційна система; інформаційні ресурси.

Постановка проблеми. Згідно з [1], "*функціональна стійкість* – це здатність системи виконувати свої функції впродовж заданого інтервалу часу за умови впливу на неї потоку експлуатаційних відмов, навмисних пошкоджень, втручання в обмін і обробку інформації та у разі помилки обслуговуючого персоналу. … *Функціональна нестійкість* – це нездатність системи відповідати сформульованим умовам функціональної стійкості". *Дисфункційним станом* називатимемо стан, у якому система стала функціонально нестійкою. Якщо виходити з визначення функціональної стійкості, то причини дисфункційних станів можуть бути зовнішні та внутрішні, злонавмисні та ненавмисні. *Функціональність* – це набір функцій, які виконує система.

Ресурси систем захисту зазвичай спрямовані на зовнішні злонавмисні причини дисфунційних станів, тому питома небезпека від внутрішніх причин може раптово стати набагато більшою, оскільки перед ними інформаційна система (ІС) повністю відкрита. До 40 % взломів банківських ІС відбувалось завдяки діям інсайдерів, тобто співробітників банків, які діяли свідомо, або несвідомо [2-4]. З іншого боку, понад 300 мобільних додатків, які розповсюджуються через офіційні магазини, містять злонавмисний код [5-7]. 71 % атак залишається невиявленим [3, 8]. Постійно тривають кібернетичні атаки на ІС силових відомств України, зокрема Міністерство оборони України, ІС державних органів та об'єктів критичної інфраструктури.

Чим більше підключено вузлів до мережі, тим більше її користь і функціональність. Водночас, чим більше підключень, тим більше ризик функціональної нестійкості через кібератаки або системні помилки. Як наслідок інциденти інформаційної безпеки (ІБ) зростають щонайменше вдвічі швидше за темпи росту інформаційних технологій (ІТ) і росту світового ВВП [2-4, 9, 10]. Основними причинами інциденців є [7] традиційне злонавмисне програмне забезпечення (ПЗ), віруси – 53 %, цільові атаки – 36 %, помилки персоналу, непередбачувані дії – 29 %, загрози від третіх сторін (постачальники, партнери) – 26 %, атаки програм – 24 %, помилки в індустріальному ПЗ – 21 %, саботаж або навмисне заподіяння фізичної шкоди ззовні – 17 %, саботаж або навмисне заподіяння фізичної шкоди співробітниками – 13 %, відмова ПЗ – 9 %. Як видно, поряд зі злонавмисними достатню частку займають і ненавмисні причини, які слід відносити до дисфункційних станів. Як би не зростали технології захисту, але видів атак завжди більше, що потребує роботи на упередження, тобто *прогнозування* розвитку атак.

Це робить актуальним розвиток засобів протидії дисфунційним станам ІС незалежно від причин походження цих станів. Під час забезпечення фунціональної стійкості ІС актуальним є розширення поняття протидії кібератакам (інцидентам ІБ) зовнішнього походження до поняття протидії дисфункційним станам ІС як зовнішнього, так і внутрішнього походження. Для дисфунційних станів внутрішнього та зовнішнього походження в більшості випадків математична формалізація є аналогічною.

Ступінь розробленості проблеми. Традиційні регресійні прогноз-моделі лише відбивають статистику того, що вже відбулось і не враховують внутрішню природу джерел небезпеки та цілей інформаційних атак. Дослідження базується на досвіді прогноз-моделювання для суміжних галузей наук, а саме медицини [11, 12], екології та техногенних катастроф [13, 14], на досвіді використання

бізнес-аналітики для систем підтримки рішень ІС медичних організацій [15].

Інциденти ІБ найчастіше пов'язують з вірусними атаками. Але цілі інформаційних атак – не виведення комп'ютера з ладу. Цілі інформаційних атак [10]: економічні збитки, удари по іміджу, підрив довіри, просування потрібного інформаційного контенту. До того ж, самі засоби захисту потребують витрат значних коштів. В існуючій літературі рекомендується утримувати видатки на захист інформації в діапазоні 10–20 %, що є занадто невизначеним діапазоном [2-4, 16]. В інших джерелах до цього додають конкретизацію існуючих діапазонів методом трьох точок (мінімум, номінал, максимум) та уточнюють рішення за допомогою усереднення методом рівномірного розподілу або бета-розподілу [17]. Фактично йдеться про діапазонні оцінки, а не про точне оптимальне рішення.

Отже управління функціональною стійкістю за критерієм мінімуму втрат від дисфункційних станів є актуальною задачею.

Метою статті є підвищення рівня захищеності мережевих інформаційних систем від дисфункційних станів завдяки розвитку методу управління функціональною стійкістю інформаційних систем на основі оптимізації видатків на захист.

Виклад основного матеріалу. Як уже зазначалося, особливістю інцидентів ІБ є те, що вони не завжди помітні (навіть не завжди заважають роботі користувачів), інколи намагаються утворити певний симбіоз із користувачем. Наприклад, спливаюча реклама або пропозиції оновлення програм, або нав'язування інсталяції програм. Проте можливий збиток від таких інцидентів може бути досить значний. Важливо, щоб жоден інцидент ІБ не залишився непоміченим, було проведено розслідування, виявлені винні, і, головне, проведені коригувальні і запобіжні заходи. Необхідна чітка процедура реєстрації та розслідування інцидентів ІБ та інформування користувачів про правила виявлення інцидентів і правила дій на випадок виявлення інцидентів [11].

Управління інцидентами ІБ не запобігає нанесенню збитку компанії. Як правило, на момент виявлення інциденту, компанія вже понесла збиток. Проте розслідування інциденту та своєчасне впровадження превентивних і коригувальних заходів знижує ймовірність його повторення і ймовірність повторного нанесення збитку.

Сумарні збитки від інцидентів ІБ складаються з таких складових: $L_{sum} = L_{inc} + L_{after} + L_{clear} + L_{it\,\mathrm{sec}}$.

Збитки безпосередньо від інциденту (атаки) – безпосереднє знищення, псування або викрадення інформації $L_{inc} = L_{inc0} \cdot \exp(-\lambda r_{it\,\mathrm{sec}})$.

Збитки внаслідок інциденту, які виникли як післядія – втрата ділової репутації, довіри, невиконання зобов'язань, неспроможність виконувати свої основні функції. Хоча остання позиція може відноситись як до п. 2, так і до п. 1 $L_{after} = k_{after} L_{inc}$.

Витрати на усунення наслідків атаки, відновлення інформаційного ресурсу та працездатності системи $L_{clear} = k_{clear} L_{inc}$.

Видатки на ІБ до виникнення інциденту $L_{it\,\mathrm{sec}} = r_{it\,\mathrm{sec}}$, де $r_{it\,\mathrm{sec}}$ – видатки на ІБ у відсотках від ІТ-бюджету організації; L_{inc0} – втрати безпосередньо від інциденту ІБ за умови нульового фінансування ІБ; λ – інтенсивність зменшення втрат від інцидентів залежності від видатків на ІБ; k_{after} – коефіцієнт втрат від наслідків інцидентів ІБ; k_{clear} – коефіцієнт видатків на усунення наслідків інцидентів ІБ.

Якщо витрачати на ІБ занадто мало, то збитки від інцидентів будуть занадто великі. Залежність збитків від рівня фінансування сфери ІБ має характер убуваючої експоненти [18] (рис. 1). Але виділимо варіанти залежно від критичності інформаційних ресурсів (ІР) для збереження функціональної стійкості організації (компанії). Під критичністю розумітимо ступінь впливу ІР на корисний ефект діяльності.

З одного боку, критичність ІР залежить від особливостей виду діяльності. Наприклад, для інженерного взводу, що риє котлован на території полігону, ІР не є критичними взагалі. У бригаді інженерних військ ІР вже помітно впливають на ефективність діяльності, оскільки дать змогу ефективно розподіляти техніку та людей зважаючи на задачі. На рівні вищого командування ефективне управління інженерною діяльністю без використання ІР практично неможливо.

З іншого боку, критичність ІР залежить від, того наскільки вони резервовані. Тобто, якщо дуже важливі ІР добре дублюються і можуть бути легко відновлені та видані користувачам навіть після атаки, то критичність основного ІР знижується. Наприклад, організація може мати дублюючі технології документообігу: паперові або на автономних ІС, які не підключені в Інтернет, а

можливо й у локальну мережу. У такій ситуації основний ІР є інформаційним буфером для видачі інформації користувачам, який веде обмін з користувачами за звичайними протоколами, а із системами резервування по особливо захищеним протоколам, за що доводиться розплачуватись деяким зниженням функціональної стійкості. Визначимо такі рівні критичності ІР (табл. 1).

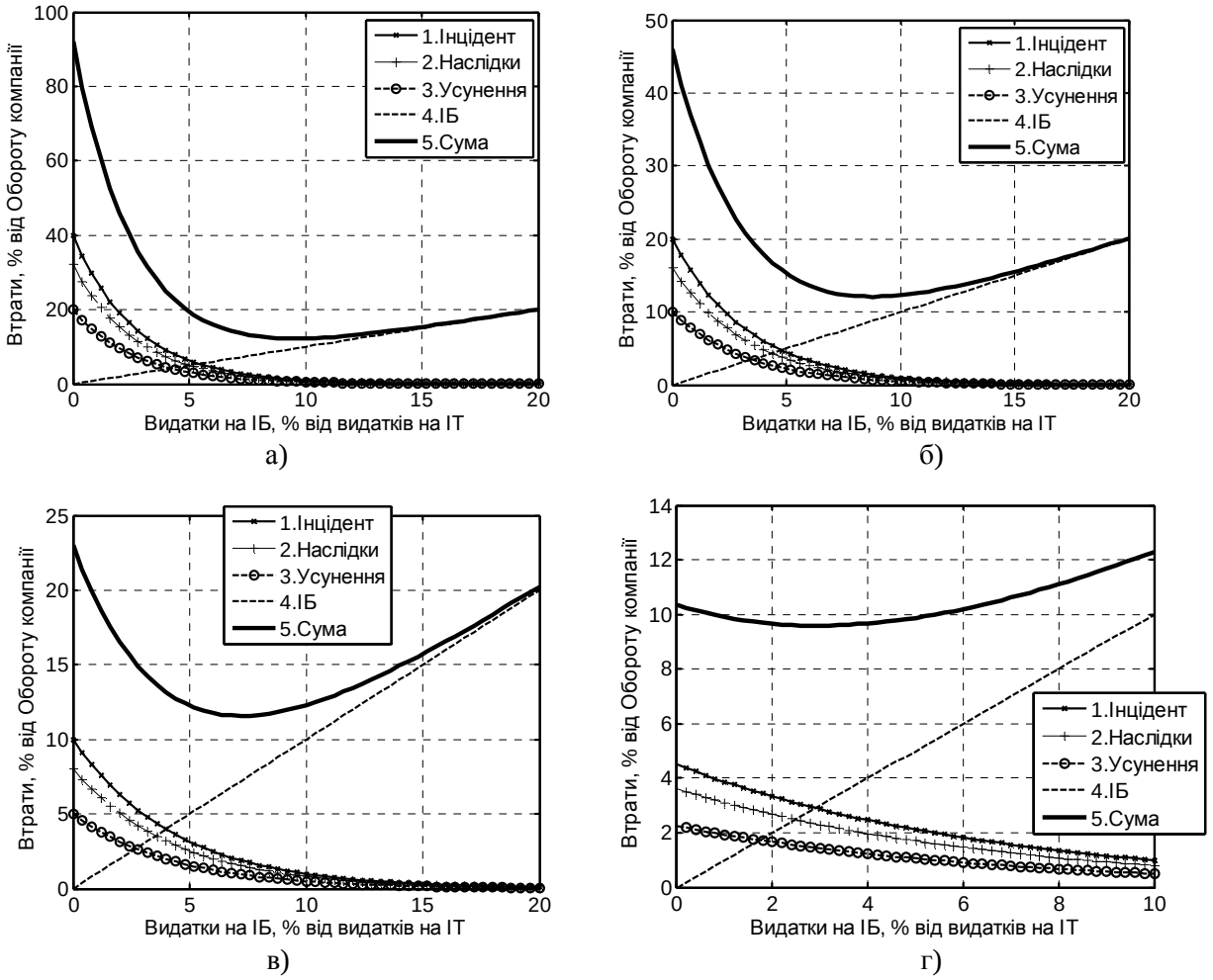

Рис. 1. Експоненційна залежність втрат від інцидентів та видатків на ІБ. Ступені критичності ІР: а) висока; б) середня в) низька б) наднизька

Таблиця 1

Рівні критичності інформаційних ресурсів

Рівень критичності ІР	Ймовірні втрати у випадку інформаційної атаки
Високий	до 100%
Середній	до 50%
Низький	до 25 %
Наднизький	близько 10%

У випадку низької критичності ІР (рис. 1 а-в) витрати на відновлення інформації можут виявитись занадто великими і величина втрат у випадку нульових видатків на ІБ сягатиме від 25 до 100 %, а в деяких випадках і перевищувати бюджет організації.

Наведені залежності показують, що існує деяке оптимальне значення видатків на ІБ. У випадку (рис. 1 г) оптимальні видатки на захист інформації знаходяться в зоні 2-4 % від загальної суми видатків на ІТ організації. У випадках (рис. 1 а-в) оптимальне значення наближується до 10 % від видатків на ІТ.

У розглянутих прикладах, які можна вважати класичними [2-4, 16, 18], не враховано, що у разі занадто малих величинах видатків на ІБ ефект від їх використання є непомітним для системи ІБ, тобто збитки від атак практично не зменшуються. Зі збільшенням видатків система ІБ починає набирати ефективність. Для врахування описаного ефекту запізнення від інвестування в ІБ замінимо експоненційну залежність у виразі для L_{inc} на S-подібну

логістичну криву $L_{inc} = \frac{L_{inc0}}{1+\exp\left[\frac{2}{T}\left(r_{it\,\sec} - \Delta r\right)\right]}$,

де T – постійна логістичної кривої (визначає нахил залежності в точці симетрії); Δr – зсув точки симетрії вздовж осі абсцис.

Найпомітнішою робота системи ІБ стає в районі 4-6 % витрат, а оптимальне значення досягається в районі 10 % від видатків на ІТ (рис. 2). До того ж, чим критичнішим є ІР, тим більше буде оптимальна величина видатків на ІБ. Такі дані відповідають досвіду побудови та використання систем ІБ в організаціях і бізнес-структурах.

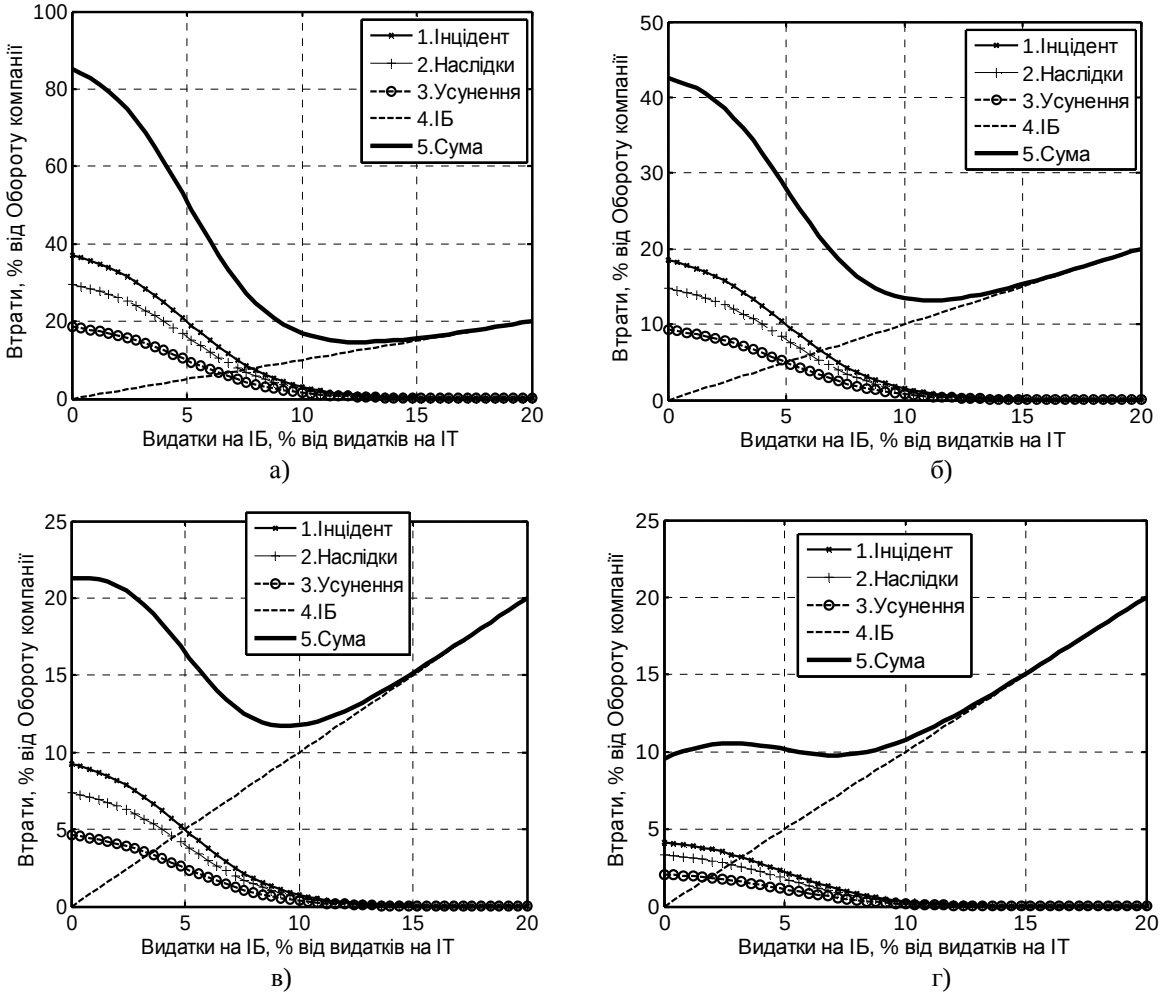

Рис.2. S-подібна (логістична) залежність втрат від інцидентів і видатків на ІБ. Ступені критичності ІР: а) висока; б) середня в) низька б) наднизька

Зауважемо, що поведінка залежностей втрат для випадків низької, середньої і високої критичності ІР мають якісно подібний характер. Картина якісно змінюється для наднизького ступеня критичності ІР, через який практично на всьому діапазоні від 0 до 9 % видатків на ІБ втрати практично однакові. Після цього сумарні втрати починають збільшуватись пропорційно видаткам на ІБ. Це пояснюється тим, що до 9 %, видатки на ІБ практично повністю компенсуються відвернутими втратами від інцидентів ІБ, а після 9 % втрати від інцидентів ІБ практично нульові і сумарні втрати визначаються виключно видатками на ІБ. Така закономірність підтверджує справедливість граничного випадку щодо витрат на ІБ: не має сенсу витрачати кошти на захист, якщо створена надійна система резервування даних. Витрати на відновлення інформації в загальнодоступному ресурсі дорівнюватиме витратам на відбиття атак. Оптимальним значенням $r_{it\,\sec}$ видатків на ІБ вважаємо видатки, які забезпечують мінімум значення L_{sum} (нижня частина відповідної кривой на рис. 2).

Як міру ступеня критичності ІР оберемо величину втрат безпосередньо від інцидентів ІБ L_{inc} та для кожного значення L_{inc} знайдемо оптимальні значення L_{sum} (рис. 3). Залежність підтверджує результати кращих практик, згідно

з якими фінансування ІБ має бути на рівні 10-20 % від ІТ-бюджету компанії [2-4, 16]. Водночас для організацій з наявністю альтернативних технологій та резервуванням інформації (критичність до 5 %) оптимальними визначені нульові або білянульові витрати. Це збігається з попередніми міркуваннями щодо (рис. 2 г)) в зоні видатків на ІБ від 0 до 9 %.

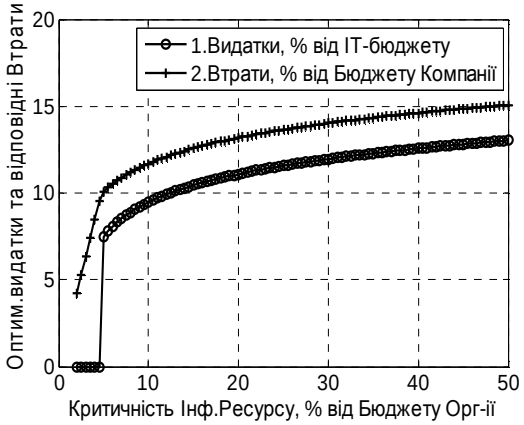

Рис. 3. Залежності рівню оптимальних видатків на ІБ для різних значень критичності ІР:

1 - видатки на ІБ (% від ІТ-бюджету компанії) оптимальні за критерієм мінімуму втрат;

2 - втрати, у випадку забезпечення оптимальних видатків на ІБ.

Відомі рекомендації щодо оптимальних витрат на ІБ в діапазоні 10-20 % недостатньо чіткі [2-4, 16]. Тим більш, що ці величини мають суттєво залежати від ступеня критичності ІР, який для кожної організації є унікальним (рис. 3). Для збільшення адекватності рекомендацій щодо витрат на ІБ також рекомендують метод трьох точок [17], який передбачає знаходження таких оцінок: 1 – мінімум, 2 – номінал, 3 – максимум, 4 – оцінка за рівномірним розподілом, 5 – оцінка за бета-розподілом. Ці рішення мають вигляд:

$1 - L_{sum1} = L_{sum}\left(r_{it\,\sec 1} = 10\%\right);$

$2 - L_{sum2} = L_{sum}\left(r_{it\,\sec 2} = 15\%\right);$

$3 - L_{sum3} = L_{sum}\left(r_{it\,\sec 3} = 20\%\right);$

$4 - L_{sum4} = \left(L_{sum1} + L_{sum2} + L_{sum3}\right)/3;$

$5 - L_{sum5} = \left(L_{sum1} + 4L_{sum2} + L_{sum3}\right)/6.$

Порівняємо ці відомі підходи щодо знаходження оптимального $L_{sumN}, N = \overline{1,5}$ з підходом запропонованим у роботі [17], L_{sumMin}. Для цього знайдемо відповідні різниці:

$1 - L_{sum1} = L_{sum1} - L_{sumMin};$

$2 - L_{sum2} = L_{sum2} - L_{sumMin};$

$3 - L_{sum3} = L_{sum3} - L_{sumMin};$

$4 - L_{sum4} = L_{sum4} - L_{sumMin};$

$5 - L_{sum5} = L_{sum5} - L_{sumMin}.$

Позитивні значення свідчитимуть про перевагу, а від'ємні про програш запропонованого підходу.

Як видно з рис. 4, практично для всіх порівнюваних відомих методів у діапазоні всіх ступенів критичності ІР запропонований метод надає виграш в більшості випадків на рівні 1-5 %, а в окремих випадках – до 16 % від бюджету компанії, що, наприклад для невеликих за світовими мірками компаній з бюджетом на рівні 100 млн дол. складає відповідно 1-5 та 16 млн дол. на рік. Тільки один з відомих методів (мінімальної оцінки) в 10 % розглянутих випадків, а саме в діапазоні ступенів критичності ІР від 11 до 16 відсотків дав такі ж результати як запропонований підхід (майже нульова різниця, рис.4).

Інциденти ІБ не єдина можлива причина втрати функціональної стійкості інформаційних систем. Іншою не менш вагомою причиною є помилки та збої в роботі, які також призводять до збитків у величині $L_{error} = k_{error} L_{inc}$.

Крім того, робота програмних систем захисту інформації потребує витрат машинних ресурсів, що також веде до збитків через зниження функціональності основного програмного забезпечення у величині $L_{unFun} = k_{unFun} \cdot r_{it\,\sec}$, де $k_{unFun}, r_{it\,\sec}$ – відповідні коефіцієнти.

З урахуванням збитків від помилок та витрачання машинних ресурсів на програмне забезпечення ІБ підсумкова залежність збитків має вигляд $L_{sum2} = L_{sum2} + L_{error} + L_{unFun}$. При цьому залежності на рис. 3, 4 приймають вигляд, як наведено на рис. 5, 6.

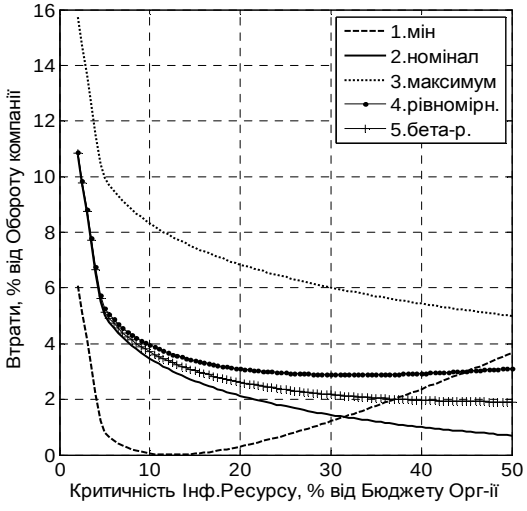

Рис. 4. Виграш запропонованого підходу

у порівнянні із відомими підходами

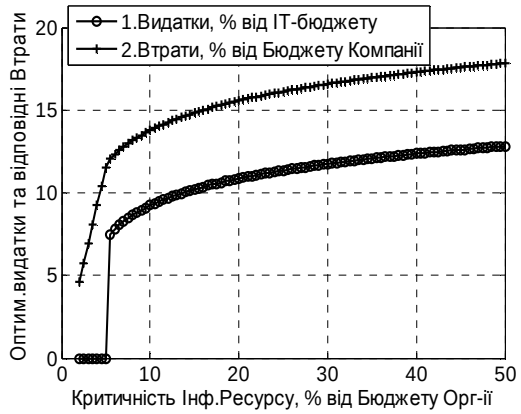

Рис. 5. Залежності рівню оптимальних видатків на ІБ для різних значень критичності інформаційних ресурсів (з урахуванням збитків від помилок та витрачання машинних ресурсів на ПЗ ІБ)

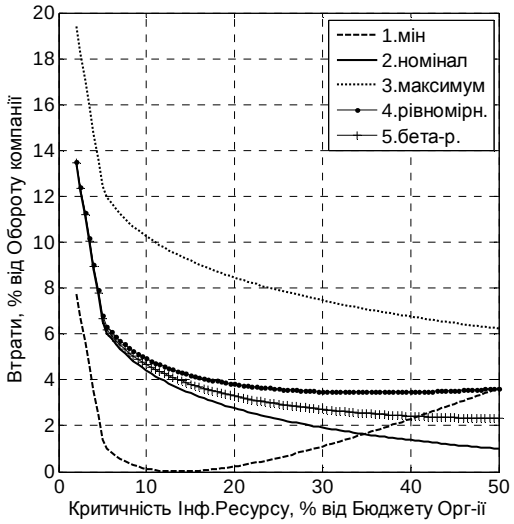

Рис. 6. Виграш запропонованого підходу у порівнянні із відомими підходами
(з урахуванням збитків від помилок та витрачання машинних ресурсів на ПЗ ІБ).

Якісно залежності зберегли свій характер, але чисельно майже всі значення зросли, що призвело до збільшення переваги запропонованого методу (рис. 6) в більшості випадків на рівні 1-6 %, а в окремих випадках виграш до 19,5 % від бюджету компанії, що, наприклад для невеликих за світовими мірками компаній з бюджетом на рівні 100 млн дол. складає відповідно 1-6 та 19,5 млн дол. на рік. Наведені залежності базувались на статистичних даних компаній PwC, Gartner [2-4]. Для прийняття правильного рішення щодо обсягів фінансування на створення системи ІБ, саме статистика інцидентів ІБ має особливу цінність для компанії, як показник ефективності функціонування системи управління ІБ. Статистику інцидентів слід регулярно аналізувати під час аудиту системи управління ІБ.

Висновки.

1. Під час розв'язання задач підвищення рівня захищеності мережевих інформаційних систем доцільно поняття комп'ютерних атак розширювати до поняття дисфункційних станів, які включають злонавмисні та ненавмисні причини інцидентів.

2. Базову експоненційну залежність збитків від дисфункційних станів залежно від величини видатків на захист доцільно замінити на адекватнішу S-подібну логістичну.

3. Рівень втрат суттєво залежеть від ступеня критичності інформаційних ресурсів для певного виду організації, яку доцільно вимірювати у величині чистих втрат безпесредньо від дисфункційного стану без урахування збитків від наслідків і витрат на усунення наслідків.

4. Інциденти інформаційної безпеки спрямовані на погіршення функціональної стійкості системи. Водночас занадто великі видатки на інформаційну безпеку відволікають інформаційні ресурси від виконання основних задач, що також погіршує функціональну стійкість. Таким чином, управління функціональною стійкістю полягає у виборі витрат на заходи інформаційної безпеки у величині, яка мінімізує загальні втрати як від можливих інцидентів ІБ, так і від занадто великих витрат на захист.

Подальші дослідження слід присвятити пов'язуванню величин витрат на захист від дисфункційних станів із конкретними технологіями захисту та розвитку методу формування оптимальних наборів засобів захисту в умовах обмежень на ресурси.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Машков О. А. Оцінка функціональної стійкості розподілених інформаційно-керуючих систем / Машков О. А., Барабаш О. В. // Фізико-математичне моделювання та інформаційні технології. – 2005. – Вип. 1. –С.157-163.
2. PwC представляет результаты глобального исследования по вопросам обеспечения информационной безопасности, перспективы на 2015 год. [електронний ресурс] // Офіційний сайт PricewaterhouseCoopers – Режим доступу http://www.pwc.ru/ru/press-releases/2015/cyber-security-press-release.html
3. The Global State of Information Security® Survey 2016. Turnaround and transformation in cybersecurity [електронний ресурс] // Офіційний сайт PricewaterhouseCoopers – Режим доступу https://www.pwc.com/gx/en/ issues/cyber-security/information-security-survey.html
4. The Global State of Information Security® Survey 2018. Turnaround and transformation in cybersecurity [електронний ресурс] // Офіційний сайт

PricewaterhouseCoopers – Режим доступу https://www.pwc.com /gx/en/issues/cyber-security/information-security-survey.html
5. Check Point Software Technologies [електронний ресурс] // Сайт Tadviser – Режим доступу http://www.tadviser.ru/index.php
6. Кибератаки / 2018/04/16 [електронний ресурс] // Сайт Tadviser – Режим доступу http://www.tadviser.ru/index.php.
7. Киберпреступность в мире. Состояние киберпреступности в различных регионах мира [електронний ресурс] // Сайт Tadviser – Режим доступу http://www.tadviser.ru/index.php
8. Healthcare cybersecurity challenges in an interconnected world. Key finding from The Global State of Information Security. Survey 2015. [електронний ресурс] // – Режим доступу http://www.pwc.ru/en/ riskassurance/publications/assets/healthcare.pdf
9. Управление киберрисками во взаимосвязанном мире. Основные результаты глобального исследования по вопросам обеспечения информационной безопасности. Перспективы на 2015 год. Январь 2015. [електронний ресурс] // Офіційний сайт PricewaterhouseCoopers - Режим доступу http://www.pwc.ru/ru/riskassurance/publications/assets/ managing-cyberrisks.pdf
10. Шевченко В. Л. Кращі світові практики управління інформаційною безпекою та їх вплив на економічну стабільність держави // Сучасний захист інформації. - №4. – Київ: ДУТ, 2015. – С. 4-9.
11. Шевченко А. В. Математична модель прогнозування динамики епідемій / Шевченко А. В., Гепко А. Л. // Профілактична медицина. – 2011. – №3(15). – с.3-6.
12. Шевченко В. Л. Оптимізаційне моделювання в стратегічному плануванні. – К.: ЦВСД НУОУ, 2011. – 283 с.
13. Шевченко А. В. Ретроспективний аналіз шляхів подолання глобальної екологічної кризи / Шевченко А. В., Громенко В. Ю. // Зб.наук.праць ЦВСД НАОУ. - 2009.- №2(40). – С. 106-114.
14. Shevchenko A. Dynamic Objects Emergency State Monitoring by Means of Smartphone Dynamic Data / Shevchenko A., Bychkov O., Shevchenko V. // 2017 14-th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM). Proceeding. – Polyana, February 21-25, 2017. – p.292-294. http://ieeexplore.ieee.org/document/7937138/ DOI: 10.1109/CADSM.2017.7916138
15. Шевченко А. В. Потенціал рішень SAP AG HEALTH CARE та DFPS для автоматизації діяльності військово-медичних закладів. / Шевченко А. В., Закалад М. А., Савицкий В. Л. // 1-й Всеукраїнський з'їзд "Медична та біологічна інформатика і кібернетика" з міжнародною участю: 23-26.06.2010: Зб.праць. – К.: НМАПО ім. П. Л. Шупика. – С. 46.
16. Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С. А., Симонов С. В. – М.: Компания АйТи ; ДМК Пресс, 2004. – 384 с.
17. A Guide to the Project Management Body Of Knowledge (PMBOK GUIDE). Sixth edition. ISBN: 978-1-62825-184-5. – Project Management Institute Inc.: Pennsylvania, USA - 2017.– 756 p.
18. Аудит та управління інцидентами інформаційної безпеки: навч.посіб. / Корченко О. Г., Гнатюк С. О., Казмірчук С. В. та ін. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 190 с.

Стаття надійшла до редакційної колегії 26.12.2018

Шевченко А. В.
Государственный университет телекоммуникаций, Киев

Управление функциональной устойчивостью информационных систем на основе оптимизации расходов на защиту

Резюме. Проанализировано состояние, направления и основные причины роста количества инцидентов информационной безопасности. Построены модели зависимости убытков от инцидентов, как функции от расходов на информационную безопасность. Найдена общая зависимость оптимальных расходов на информационную безопасность в зависимости от уровня критичности информационных ресурсов организации.

Ключевые слова: инциденты; информационная безопасность; функциональная устойчивость; информационная система; информационные ресурсы.

A. Shevchenko
State University of Telecommunication, Kyiv

Managing the functional stability of information systems based on defense cost optimization

Resume. The state, directions and main reasons for the increase in the number of information security incidents are analyzed. The models of dependence of losses on incidents, as a function of the costs of information security, are constructed. The general dependence of the optimal expenditures on information security depending on the level of critical information resources of the organization has been found.

Keywords: incidents; information security; functional stability; optimums; expenditures; information system; information resources.