

УДК 004.056:654.026

DOI: 10.18372/2073-4751.72.17457

Гнатюк С.О., д.т.н.,
orcid.org/0000-0003-4992-0564,**Сидоренко В.М.**, к.т.н.,
orcid.org/0000-0002-5910-0837,**Березовий І.Р.**,
orcid.org/0000-0003-0015-8329,**Сидоренко С.Ю.**,
orcid.org/0000-0002-7170-123X,**Тараненко К.О.**

МОДЕЛЬ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВЗАЄМОЗАЛЕЖНИХ КРИТИЧНИХ ІНФРАСТРУКТУР

Національний авіаційний університет

s.gnatyuk@nau.edu.ua,

v.sydoenko@ukr.net,

i.berezovyi@gmail.com

Вступ

Сьогодні критичні інфраструктури (КІ) суттєво відрізняються у різних державах, проте суттєвою об'єднуючою ознакою є тісний взаємозв'язок та складна взаємозалежність від низки (безлічі) інформаційно-комунікаційних технологій (ІКТ). Інфраструктура визначається як мережа взаємозалежних систем і процесів, які тісно співпрацюють і постійно виробляють та розповсюджують безперервний потік товарів і послуг, необхідних для розвитку суспільства. КІ держави багато в чому взаємопов'язані та взаємозалежні, як фізично, так і через низку ІКТ. Це призводить до того, що збої у певній інфраструктурі прямо чи опосередковано впливають на інші об'єкти інфраструктури, та можуть нанести шкоду цілому географічному регіону, і мати суттєві наслідки для економіки держави чи навіть світової економіки [1-2].

Безпека держави, а також якість життя її громадян, залежать від безперервної надійної роботи комплексу складних взаємозалежних критичних інфраструктур (ВКІ), що включають транспорт, електроенергію, нафту, газ, телекомунікації та аварійно-рятувальні служби. Збій в одній інфраструктурі може швидко та суттєво впливати на іншу. Сучасні інфраструктури

майже повністю залежать від ІКТ та інтернету, і часто для їх надійної роботи необхідно бути підключеними одна до одної через електронні канали зв'язку.

Крім того, одна технологія, яка дозволяє передавати інформацію по всьому світу одним «клацанням миші», може бути використана для порушення життєво важливих систем, включаючи потік електроенергії або води, та служб екстреної допомоги. І поки ці технології дозволяють досягти величезних приростів ефективності, вони одночасно створюють нові вразливі місця. Зазначені уразливості свідчать про наявність важливого наукового завдання щодо оцінювання ефективності функціонування систем інформаційної безпеки (ІБ) ВКІ.

Аналіз останніх досліджень та публікацій

Національна та економічна безпека залежать від КІ та ІКТ, що їх постійно підтримують. З метою забезпечення їх надійності та охорони створюються спеціальні комітети та встановлюються вимоги до кожної галузі інфраструктури.

Діяльність цих комітетів спрямована на захист системи проти ворожого проникнення, або комп'ютерних атак, які можуть спричинити збій в основних інфраструктурах.

Відповідно до [3,4], основні інфраструктури можна умовно розділити на дві основні категорії:

1. Інфраструктури, діяльність яких базується виключно на ІКТ, посиляючись на більшість фінансових інфраструктур;

2. Інфраструктури, що працюють через системи SCADA. Це спеціальна система диспетчерського контролю та збору даних для об'єктів критичних інфраструктур (ОКІ), таких як електроенергія, вода, газ, паливо, зв'язок, транспорт тощо. Ці системи використовують датчики надання інформації в режимі реального часу і дозволяють контролювати та впроваджувати операційні зміни.

Ще однією придатною моделлю для опису поведінки критичної інфраструктури та взаємозалежності між ними є модель визначення інфраструктурних систем як комплексних адаптивних систем (CAS) [5].

Ці системи є складними, оскільки вони різноманітні та містять велику кількість взаємопов'язаних компонентів. Вони адаптивні, тому дозволяють приймати правильні рішення компонентами системи, змінюватись у відповідь на інформацію від інших компонентів і на зовнішні втручання.

Проведемо детальний аналіз існуючих методів оцінювання ефективності функціонування систем ІБ ВКІ.

У роботах [6-8] представлено процесно-статистичний підхід оцінювання ефективності. У результаті виконання якого, можливо отримати гістограму розподілу та інтегральний відсоток розподілу сумарного значення попереджених втрат. Ці значення дозволяють оцінити ймовірність конкретного значення у будь-якій вибраній точці або у заданому інтервалі. Цю ймовірність, з конкретним значенням суми попереджених втрат, можна вважати в обґрунтуванні ефективності заходів щодо підвищення ІБ з гарантійною ймовірністю.

Оптимізаційний метод оцінювання ефективності, описаний у [9] полягає у складенні сценаріїв розвитку небезпеки системи у вигляді графу, що є логіко-

ймовірною моделлю відображення функціонування системи. Це дводольний граф $G(A,U)$, вершини множини A відповідають апаратним та програмним засобам захисту, а вершини множини U – відповідним інформаційним загрозам. Кожен елемент (вершина) множини A характеризується ціною і ефективністю щодо нейтралізації інформаційних загроз. Кожній вершині множини U присвоюється вага, що дорівнює вартості, яка відповідає СЗІ, а кожній дузі – вага $p(i,j)=\{1,0\}$. Кінцева подія визначає небезпечний стан системи.

У роботі [10], представлено підхід діючих та запланованих заходів захисту функціонуючих систем КІ, який описує процес перевірки функціональності та правильності роботи діючих систем. Якщо передбачається, що будь-який засіб захисту інформації функціонує правильно, але це не підтверджується у процесі здійснення ділових операцій, то функціонування його може стати джерелом можливої вразливості. За результатами роботи методу складають перелік діючих та запланованих заходів захисту із зазначенням статусу їх реалізації та використання. Остаточне визначення ризику здійснюється шляхом розрахунку показника ефективності. За результатами цього порівняння робиться висновок, що якщо ризик допустимим, то наступним етапом стає оформлення документів по оцінці ефективності системи захисту інформації. Якщо ризик перевищує допустимий рівень, то необхідно коригування заходів захисту, після чого необхідно ще раз пройти процедуру розрахунку потенційного ризику безпеки зв'язку.

Запропонована у роботах [11,12] модель оцінювання ефективності банківських інформаційних ресурсів (БІР) базується на розрахунку комплексного показника ефективності інвестицій, що виділяються на забезпечення безпеки БІР і дисконтуванні майбутніх грошових надходжень і витрат. Запропонований підхід на основі комплексного показника ефективності інвестицій, що дозволяє відкрити новий (емерджентний), з позицій безпеки, та ефективний з позицій витрачених коштів

підхід до побудови діючих і перспективних систем безпеки БІР [12].

У табл. 1 систематизовано результати проведеного аналізу методів оцінювання ефективності функціонування систем ІБ за такими критеріями:

1. ясність формалізації (чіткість і зрозумілість математичних розрахунків);
2. простота реалізації (відсутність надскладних процедур);
3. гнучкість та універсальність (можливість зміни параметрів та застосування у різних галузях);
4. об'єктивність (можливість незалежного оцінювання).

Таблиця 1. Аналіз методів оцінювання ефективності функціонування систем ІБ

Підхід	1	2	3	4
Процесно-статистичний підхід оцінювання ефективності	+	-	+	+
Оптимізаційний метод оцінювання ефективності	-	+	+	-
Підхід діючих та запланованих заходів захисту функціонуючих систем КІ	-	-	-	+
Модель оцінювання ефективності систем БІР	+	+	-	+

Таким чином, з табл. 1 видно, що найбільш придатною за усіма параметрами є модель оцінювання ефективності БІР, яка розраховує ефективність, враховує зміну інвестицій в безпеку з плином часу, але орієнтована (в більшості) тільки на банківську безпеку та безпеку БІР.

Мета цієї статті – розроблення і дослідження моделі оцінювання ефективності функціонування систем ІБ ВКІ.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

1. Проаналізувати існуючі підходи до оцінювання ефективності функціонування систем ІБ для визначення їх переваг та недоліків;
2. Розробити модель оцінювання ефективності функціонування систем ІБ ВКІ, для можливості комплексного визначення основних показників інвестування у систему ІБ та забезпечення заданого рівня її безпеки;

3. Дослідити експериментально розроблену модель оцінювання ефективності функціонування систем ІБ для її верифікації.

Модель оцінювання ефективності функціонування систем ІБ ВКІ

Модель оцінювання ефективності функціонування систем ІБ ВКІ, складається з чотирьох етапів, а саме:

1. Визначення зв'язків;
2. Визначення з'єднань;
3. Розрахунок ефективності та продуктивності системи;
4. Оптимізація інвестицій [1-2].

Розглянемо їх більш детально.

Етап 1. Визначення зв'язків

Для представлення системи ВКІ будемо використовувати теорію графів, де вузли графу будуть представляти ОКІ, а дуги – компоненти інфраструктури або зв'язки між ними. Слід зауважити, що дуги графу мають можливість змінюватись та навіть бути невизначеними. Крім того, певні можливості одного компонента або підсистеми можуть бути пов'язані з продуктивністю кількох інших компонентів або підсистем і вихід з ладу певної ланки може спричинити такі самі, або навіть більш серйозні труднощі.

Нехай мережа доставки ОКІ містить окремих постачальників, маркованих S1 і S2. ОКІ, що потрапляє у розподільчу мережу від постачальника S1, надходить через вузол DS1. Аналогічно ОКІ, що надходить у розподільчу мережу від постачальника S2, надходить через вузол DS2. Існує чотири різні попити на ОКІ, що обслуговуються цією мережею, два з яких будемо маркувати як E1 та E2. Шляхом поділу об'єктів, що генерують, на два вузли і сполучну дугу (наприклад, E1 і G1) можна представити «відмову вузла» (часткова або повна втрата генератора) як втрату ємності на сполучній дузі. Значення попиту ОКІ (протягом кожного періоду) визначаються на вузлах D1, D2, L1 і L2. Номери поряд зі зв'язками в мережі становлять номінальну пропускну здатність цих з'єднань.

Етап 2. Визначення з'єднань

Устаткування SCADA відстежує, контролює та регулює транспортування системи ОКІ в з'єднаннях $a \rightarrow b$, $b \rightarrow c$, $c \rightarrow d$ та $d \rightarrow e$. Тепер припустимо, що SCADA має дві основні підсистеми. Одна підсистема підтримує зв'язки $a \rightarrow b$ та $b \rightarrow c$, а друга – $c \rightarrow d$ та $d \rightarrow e$. Зміни пропускної спроможності згодом можуть включати випадкові збої (що знижують потужність дуги), або ремонтні роботи невизначеної тривалості (які відновлюють працездатність). Для визначення станів зв'язку, що відповідають різним рівням потужності, використаємо марківські та напівмарківські процеси [13] для представлення переходів стану у час.

Стан кожної із двох підсистем SCADA представлений двійковою випадковою змінною, де «0» вказує на зменшений стан (часткова втрата функціональності) та «1» вказує на повну функціональність. Оскільки зв'язки $a \rightarrow b$ та $b \rightarrow c$ керуються однією підсистемою SCADA, зміни їх потужності, що визначаються станом системи SCADA, відбуваються разом, створюючи кореляцію між ними. Аналогічно і зі зв'язками $c \rightarrow d$ і $d \rightarrow e$. Оскільки можливості систем посилення $a \rightarrow b$, $b \rightarrow c$, $c \rightarrow d$ та $d \rightarrow e$ залежать від стану системи SCADA, визначення станів залежить від стану відповідної підсистеми SCADA.

Етап 3. Розрахунок ефективності та продуктивності системи

Оцінка імовірнісного розподілу ОКІ, що поставляється на D1 і D2, L1 і L2, має вирішальне значення для розуміння якості послуг, які можуть бути запропоновані клієнтам. Розуміння «часу відновлення» дає уявлення про надійність системи.

Розглянемо задачу нескінченного горизонтального узагальненого мережевого потоку з набором вузлів N та набором дуг A . Припустимо $c_t(i, j)$ – ємність дуги $(i, j) \in A$ в період t .

Нехай $C_t = (c_t(i, j)) \in E$ і $C = \{C_t\} \in E^\infty$, де E простір стану для ємності на всіх зв'язках в періоді t . Припустимо, що C є напівмарківським процесом з імовірнісною мірою $\mu(C, \theta)$.

Нехай D – вимоги до кожного вузла попиту у кожний період. Припустимо, що f – показник продуктивності, що визначається на E^∞ . У проміжному аналізі f – розподіл часу для «відновлення». В аналізі стійкого стану f – розподіл ймовірностей для продукту, що поставляється на кожен вузол попиту. Існує можливість оцінити розподіл ймовірності та час відновлення за допомогою моделювання. Процедура створення спостереження з цього розподілу виглядає таким чином:

1. Нехай $i = 1$; тоді для кожного з'єднання припустимо, що ємність щойно досягла найнижчого можливого стану.

2. З огляду на пропускну спроможність кожної ланки, вирішимо узагальнену проблему потоку для визначення попиту, задоволеного в кожному місці за умови, що всі вимоги однаково важливі.

3. Нехай $i = i + 1$.

4. Якщо всі вимоги виконано зупиняємось, а значення i буде відображенням кількості періодів, необхідних для відновлення.

5. Відновлюємо кожен стан посилення на основі пов'язаного стохастичного процесу та переходимо до кроку 2.

Оскільки деякі стохастичні процеси мають можливість переходу, яка досить мала і досить довга, ймовірно, буде потрібно багато реплікацій. Для подолання цієї проблеми можна використовувати вибірку, що має важливе значення. Основна ідея використання вибірки важливості полягає у виборі альтернативних перехідних матриць та розподіл часу утримання, які є більш обчислювально вигідними, але «коригують» результати з використанням відносної ймовірності спостереження за початковими параметрами.

Етап 4. Оптимізації інвестицій

Інвестиційні можливості, які можуть підвищити ефективність, можуть бути представлені у марківських моделях як зміни у перехідних матрицях. Адже перехідна матриця для каналу зв'язку в мережі створює загальний вплив на продуктивність системи в цілому, і цей ефект можна оцінити за допомогою моделювання.

У загальному математичному сенсі, якщо C є марківським або напів-марківським процесом, що залежить від будь-якого параметра θ , він має міру ймовірності $\mu(C, \theta)$, яка визначає ймовірності системи, що займає різні стани. Якщо система має показник продуктивності $g(C)$, модель моделювання може розглядатися як побудова оцінки очікуваної продуктивності для даного θ : $f(\theta) = E_{\theta}[g(C)] = \int g(C)\mu(dC, \theta)$.

Для оцінювання ефективності будемо використовувати наступний вираз:

$$a(\theta) = \sum g(C)\pi(C, \theta),$$

де $g(C)$ – ймовірність того, що всі вимоги будуть задоволені, а $\pi(C, \theta)$ – це ймовірність сталого стану при θ .

Процедура виглядає так:

Крок 1: Потрібно розрахувати 1000 вибірових шляхів системи по 1000 періодів кожен, використовуючи перехідні матриці для кожної ланки, які схожі на ті, що в базовій конфігурації системи, але дозволяють більш «ефективне моделювання». Нехай θ є стохастичними процесами, вибраними для кожного посилення. Потрібно розрахувати ймовірність, за якої всі вимоги задовольняються при θ , і нехай це значення буде P^* .

Крок 2: Необхідно визначити зв'язки, для яких є достатньо коштів, щоб реалізувати наступні додаткові інвестиції. Якщо немає зв'язків – потрібно зупинитися.

Крок 3: Для кожної з ланок, зазначених у кроці 2, потрібно окремо розрахувати ймовірності того, що всі вимоги можуть бути задоволені, якщо будуть зроблені додаткові інвестиції за посиленням. Кожен розрахунок вимагає «коригування» 1000 маршрутів вибірки, визначених на етапі 1, на основі «функції важливості» для з'єднань.

Крок 4: Потрібно зробити додаткові інвестиції за посиленням, що призводить до найбільшого збільшення ймовірності того, що всі вимоги можуть бути задоволені, якщо це збільшення є позитивним. Якщо покращення буде позитивним, треба оновити P^* , зменшити бюджет, доступний з урахуванням цих інвестицій, оновити

набір стохастичного процесу на посиленнях θ і перейти до кроку 2; інакше – потрібно зупинитися.

Запропонована модель оцінювання ефективності функціонування систем ІБ, яка за рахунок представлення ВКІ у вигляді марківських та напівмарківських процесів, введення змін в простір станів та матриці переходів, дозволяє оптимізувати витрати та інвестиції у систему ІБ при одночасному забезпеченні заданого рівня її безпеки.

Експериментальне дослідження моделі

Етап 1. Для експериментального дослідження запропонованої моделі розглянемо невеликий приклад двох ВКІ – мережу розподілу газу та мережу виробництва / розподілу електроенергії [1-2]. Газорозподільна мережа підтримується диспетчерським керуванням та системою збору даних.

Комбінована газоелектрична мережа показана на рис. 1. Він містить два окремих постачальника, маркованих $S1$ і $S2$. Газ, що у розподільчу мережу від постачальника $S1$, надходить через вузол $DS1$. Аналогічно газ, що надходить у розподільчу мережу від постачальника $S2$, надходить через вузол $DS2$. Існує чотири різні попиту на газ, що обслуговуються цією мережею, дві з яких є електростанціями ($E1$ та $E2$). Будь-яка електростанція може обслуговувати електричне навантаження на $L2$, але тільки один із генераторів може обслуговувати електричне навантаження на $L1$. Шляхом поділу об'єктів, що генерують, на два вузли і сполучну дугу (наприклад, $E1$ і $G1$) можливо представити «відмову вузла» (часткова або повна втрата генератора) як втрата ємності на сполучній дузі.

Значення попиту газу та електроенергії (протягом кожного періоду) фіксуються на вузлах $D1$, $D2$, $L1$ і $L2$. Номери поряд зі зв'язками в мережі становлять номінальну пропускну здатність цих з'єднань.

Етап 2. Відомо, що SCADA має дві основні підсистеми. Одна підсистема

підтримує зв'язки $a \rightarrow b$ та $b \rightarrow c$, а друга – $c \rightarrow d$ та $d \rightarrow e$. На рис. 1 показані можливості встановлення зв'язків, які вважаються детермінованими. Крім того, було визначені стохастичні процеси для тих ланок, які розглядаються як такі, що мають невизначену ємність. Наприклад, посилання $S1 \rightarrow DS1$ може мати ємність 90, 95, 100 або 105. Передбачається, що еволюція потужностей газотранспортних магістралей є напівмарківським процесом, а інші зв'язки характеризуються марківськими процесами. Спостереження за цими розподілами округляються визначення кількості періодів, протягом яких здійснюється процес.

Стан кожної із двох підсистем SCADA представлений двійковою випадковою змінною, де 0 вказує на зменшений стан (часткова втрата функціональності) та 1 вказує на повну функціональність. Отже, якщо частина системи SCADA, яка забезпечує підтримку зв'язків $a \rightarrow b$ та $b \rightarrow c$, знаходиться в зменшеному стані, то найвищий стан ємності становить 250 при зв'язку $a \rightarrow b$ замість 300.

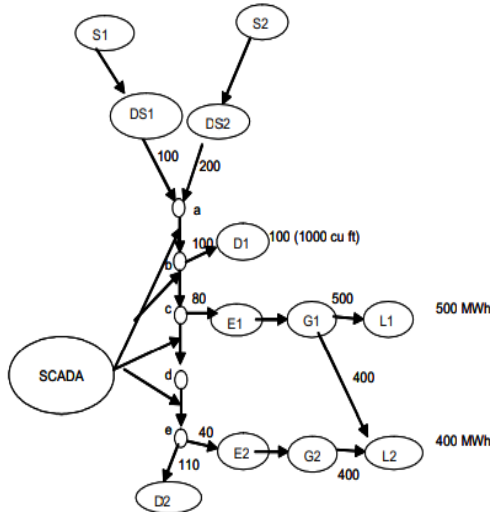


Рис. 1. Представлення мережі ВКІ

Етап 3. Оцінювання імовірного розподілу газу, що поставляється на D1 і D2 і електроенергії, що поставляється на L1 і L2, має вирішальне значення для розуміння якості послуг, які можуть бути запропоновані клієнтам. А показник f містить чотири ймовірні розподіли.

На рис. 2 показано розподіл ймовірності тимчасово відновлення з

урахуванням 1000 реплікацій. Середній час відновлення становить 10,6 періодів, але існує близько 5% шанс, що це займе 20 або більше періодів, і в одному експерименті він становив 36 періодів для відновлення системи. Через структуру аналізу легко визначити умови, що породжують кожне спостереження для відновлення часу. Така інформація, ймовірно, буде особливо цінною для директивних органів, які прагнуть підвищити ефективність системи.

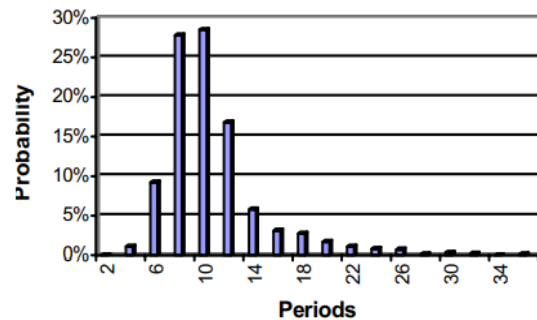
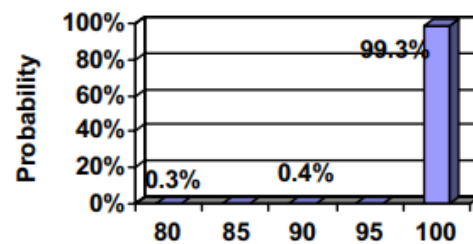
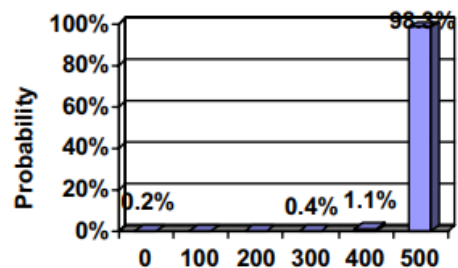


Рис. 2. Представлення часу відновлення функціональності системи ВКІ

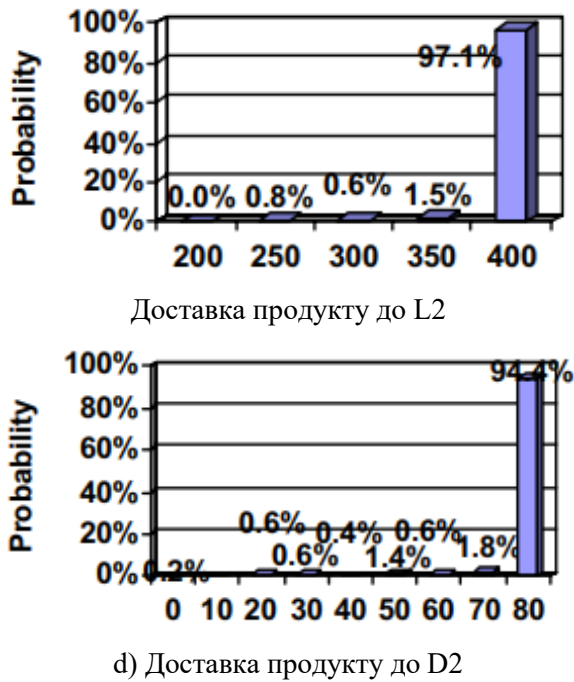
Далі, використовуючи алгоритм описаний на Етапі 3, було оцінено стаціонарний розподіл ймовірностей для продукту, який постачається у кожне місце попиту. Рис. 3. ілюструє розподіл ймовірностей для продуктів, що постачаються на кожен вузол попиту, на основі 1000 реплікацій схеми стаціонарної вибірки.



Доставка продукту до D1



Доставка продукту до L1



d) Доставка продукту до D2

Рис. 3. Ймовірності розподілу доставки продукту у стабільному функціонуванні

Також, рис. 3 відображає розподіл ймовірностей для продуктів, що поставляються на кожен вузол попиту (якщо резервуар для зберігання недоступний), на основі 1000 реплікацій стаціонарної вибірки. Частка періодів, у яких вимоги до різних «навантажувальних вузлів» системи варіюються від близько 94% до 99%. У цілому, важче задовольнити попит на D2, чим на D1 через невизначеність, пов'язану зі зв'язками $b \rightarrow c$, $c \rightarrow d$ і $d \rightarrow e$.

Етап 4. Інвестиційні можливості, які можуть підвищити ефективність, можуть бути представлені у марківських моделях як зміни у перехідних матрицях. Наприклад, для того щоб підвищити надійність частини обладнання, і уявити це покращення як зниження ймовірності введення несправностей у марківській моделі за потужністю. Ця альтернативна перехідна матриця для каналу зв'язку в мережі і загальний вплив на продуктивність системи можна оцінити за допомогою моделювання. Заміна старої перехідної матриці також пов'язана із витратами на її покращення. Таким чином, завдання оптимізації інвестицій полягає у визначенні того, які інвестиції (зміни в конкретних перехідних матрицях) слід вкладати, щоб максимально

підвищити ефективність системи, з урахуванням бюджетних обмежень на загальні понесені витрати.

Розглянемо детально, які можуть бути зроблені інвестиції для підвищення надійності доставки газу від обох постачальників, системи SCADA, газопроводів, а також генераторів. Припустимо, що за 100 тисяч \$, інвестовані на посилення, найнижчий стан ємності видаляється і можливість переходу в цей стан додається до тих, що для наступного нижчого стану. Для кожного послідовно видаленого стану вартість складає 150, 200, 250, 300, 350 та 400 тисяч \$ відповідно. Інвестиції за посиленням мають бути зроблені правильно. Наприклад, щоб забезпечити щонайменше 100 000 кубічних футів газу в постачальника 1, необхідно інвестувати 250 тисяч \$. Метою оптимізації витрат є досягнення компромісу, коли забезпечена умова максимізації ймовірності стійкого стану, що всі вимоги виконані.

Запропонований порядок інвестицій полягає в тому, щоб спочатку забезпечити надійність поставок газу від постачальника 2, потім інвестувати в газопроводи $c \rightarrow d$ та $d \rightarrow e$, а потім у лінії електрогенерації $E1 \rightarrow G1$ та $E2 \rightarrow G2$.

Найбільш значним поліпшенням загальної надійності системи є підвищення надійності поставок газу від постачальника 2. Без такого постачання збільшення пропускної спроможності системи надалі «на нижньому рівні» є неефективним. Наступні інвестиції в газопроводи та виробництво електроенергії можуть трохи підвищити надійність системи, але оптимізація вказує на газопостачання як на найважливішу інвестиційну галузь.

Цей приклад є досить простим і водночас складним, що дозволило ілюструвати процеси у набагато більших складних реальних мережах.

Як показав проведений експеримент, використання запропонованої моделі дозволяє комплексно оцінювати основні показники інвестування у забезпечення безпеки ВКІ держави із урахуванням бюджетних обмежень на загальні понесені витрати.

Висновки

У роботі було проведено аналіз існуючих підходів до оцінювання ефективності функціонування ВКІ та визначено їх основні переваги та недоліки. Встановлено, що найбільше переваг має модель оцінювання ефективності БІР, яка розраховує ефективність, враховує зміну інвестицій в безпеку з плином часу, але орієнтована в більшості тільки на банківську безпеку та безпеку БІР.

Розроблено модель оцінювання ефективності функціонування систем ІБ, яка за рахунок представлення ВКІ у вигляді марківських та напівмарківських процесів, введення змін в простір станів та матриці переходів, дозволяє оптимізувати витрати та інвестиції у систему ІБ при одночасному забезпеченні заданого (необхідного) рівня її безпеки.

Крім того, в роботі проведено експериментальне дослідження згаданої моделі, що підтвердило її ефективність комплексно оцінювати основні показники інвестування у забезпечення безпеки ВКІ держави із урахуванням бюджетних обмежень на загальні понесені витрати.

Література

1. *Nozick L., Turnquist M., Jones D., Davis J., Lawton C.* Assessing the Performance of Interdependent Infrastructures and Optimizing Investment. Proceedings of the 37th Hawaii International Conference on Systems Sciences, Jan. 2004.
2. *Xu N., Nozick L.K., Turnquist M.A., Jones D.A.* Optimizing Investment for Recovery in Interdependent Infrastructure, 2007. 40th Annual Hawaii International Conference on System Sciences (HICSS'07), Waikoloa, HI, USA, 2007. – P. 112-112.
3. *Boyer, Stuart A.* SCADA Supervisory Control and Data Acquisition. – USA: ISA – International Society of Automation, 2010. – 179 p.
4. *Abbas H.A., Mohamed A.M.* Review in the design of web based SCADA systems based on OPC DA protocol. International Journal of Computer Networks, February, 2011. – Vol. 2. – No. 6. – P. 266-277.
5. *Rinaldi S., Peerenboom J., Kelly T.* Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine, 11- 25, December 2001.
6. *Mussington D.* Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development. RAND:Science and Technology Institute, Santa Monica, CA, 2002. – 29 p.
7. *Petit F., Wallace K., Phillips J.* An Approach to Critical Infrastructure Resilience. The CIP Report, Center for Infrastructure Protection and Homeland Security, George Mason University School of Law, January, 2014. – Vol. 12. – No. 7. – P. 17-20.
8. *Phillips J.A., Bassett G.W., Buehring W.A., Carlson J.L., Whitfield R.G., Peerenboom J.P.* A Framework for Assessing Infrastructure Risk, M4-I Resilience Evaluation Approaches for the Analysis of Complex Systems, Risk Analysis: Advancing Analysis, Society for Risk Analysis, 2012.
9. *Gürkan G., Ozge Y., Robinson S.* Sample Path Optimization in Simulation. Proceedings of the 1994 Winter Simulation Conference, December 11-14 1994. – P. 247-254.
10. *Abbas H.A., Mohamed A.M.* Review in the design of web based SCADA systems based on OPC DA protocol. International Journal of Computer Networks, February, 2011. – Vol. 2. – No. 6. – P. 266-277.
11. *Євсєєв С., Король О.* Комплексний показник ефективності інвестицій в безпеку банківської інформації на основі синергетичної моделі загроз. VI Міжнародна наукова конференція “Інформація, комунікація, суспільство 2017”, Славське, 2017. – С. 18-19.
12. *Євсєєв С.П.* Методологія побудови системи безпеки банківських інформаційних ресурсів. Кваліфікаційна наукова праця на правах рукопису. – К.: НАУ, 2018.
13. *Limnios N., Oprisan G.* Semi-Markov Processes and Reliability. – Birkhäuser, Boston, 2001.

Гнатюк С.О., Сидоренко В.М., Березовий І.Р., Сидоренко С.Ю., Тараненко К.О.

МОДЕЛЬ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВЗАЄМОЗАЛЕЖНИХ КРИТИЧНИХ ІНФРАСТРУКТУР

Сьогодні критичні інфраструктури націй суттєво відрізняються один від одного у різних країнах, проте безперечним об'єднуючим фактором є тісний взаємоз'язок та складна взаємозалежність від безлічі інформаційно-комунікаційні технології. Безпека нашої країни, а також якість життя її громадян залежить від безперервної надійної роботи комплексу складних взаємозалежних інфраструктур, включаючи транспорт, електроенергію, нафту, газ, телекомунікації та аварійно-рятувальні служби. А збій в одній інфраструктурі може швидко та суттєво впливати на іншу. Сучасні інфраструктури майже повністю залежать від нових інформаційних технологій та інтернету, і часто для надійної роботи яких необхідно бути підключеними одна до одної через електронні, інформаційні зв'язки. І поки ці технології дозволяють досягти величезних приростів у ефективності, вони також створюють нові вразливі місця. Таким чином виникає необхідність розробки нових моделей та методів для забезпечення стабільного функціонування взаємозалежних критичних інфраструктур (ВКІ). У роботі представлено модель оцінювання ефективності функціонування систем ІБ, яка за рахунок представлення ВКІ у вигляді марківських та напівмарківських процесів, введення змін в простір станів та матриці переходів, дозволяє оптимізувати витрати та інвестиції у систему ІБ при одночасному забезпеченні заданого рівня її безпеки. Крім того, було проведено експериментальне дослідження запропонованої моделі. Використання даної моделі, дозволяє комплексно оцінювати основні показники інвестування в забезпечення безпеки ВКІ держави, з урахуванням бюджетних обмежень на загальні понесені витрати.

Ключові слова: критична інфраструктура, взаємозалежні критичні інфраструктури, об'єкти критичної інфраструктури, ефективність, модель оцінювання ефективності, оптимізація інвестицій, рівень безпеки.

Gnatyuk S.O., Sydorenko V.M., Berezovyi I.R., Sydorenko S.Yu., Taranenko K.O.

MODEL FOR ASSESSING THE EFFICIENCY OF INFORMATION SECURITY SYSTEMS FUNCTIONING IN INTERDEPENDENT CRITICAL INFRASTRUCTURES

Today, the critical infrastructures of nations differ significantly from one another in different countries, but the indisputable unifying factor is the close relationship and complex interdependence of a multitude of information and communication technologies. The security of our country, as well as the quality of life of its citizens, depends on the continuous reliable operation of a complex of interdependent infrastructures, including transportation, electricity, oil, gas, telecommunications and emergency services. And a failure in one infrastructure can quickly and significantly affect another. Modern infrastructures are almost completely dependent on new information technologies and the Internet, and often for their reliable operation they need to be connected to each other through electronic, informational communications. And while these technologies allow for huge gains in efficiency, they also create new vulnerabilities. Thus, there is a need to develop new models and methods to ensure the stable functioning of interdependent critical infrastructures (ICI). The paper presents a model for assessing the effectiveness of IS systems functioning, which, due to the representation of ICI in the form of Markov and semi-Markov processes, introduction of changes in the state space and transition matrix, allows to optimize costs and investments in the IS system while simultaneously ensuring a given level of its security. In addition, an experimental study of the proposed model was conducted. The use of this model makes it possible to comprehensively evaluate the main indicators of investment in ensuring the security of ICI of the state, taking into account budgetary restrictions on the total costs incurred.

Keywords: critical infrastructure, interdependent critical infrastructures, critical infrastructure objects, efficiency, efficiency evaluation model, investment optimization, security level.