Інформаційні та телекомунікаційні системи та технології, захист інформації

УДК 004.056, 004.75 DOI: 10.20535/2312-1807.2017.22.2.94613
Кучернюк П. В., к.т.н., OrcID 0000-0001-6381-0156
e-mail kuchernuk@kpi.ua
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Довгаль А. О., OrcID 0000-0002-4035-110X
e-mail dovgal.andrey@ua.sika.com
компанія «Сіка»

МОДЕЛЬ ЗАГРОЗ БЕЗПЕКИ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ НА ОСНОВІ РЕГРЕСІЙНОГО АНАЛІЗУ

Засобами регресійного аналізу з використанням багаторівневої класифікації загроз, яка базується на моделі OSI, розроблена математична модель загроз безпеці інформаційно-комунікаційних систем. Розглянута постановка задачі та показано, як з теоретичної моделі отримати апроксимаційне рівняння регресії, яке може бути використано для подальшого прогнозування впливу можливих атак на стан мережі. Запропонована формалізована процедура розрахунку коефіцієнтів регресії та на прикладі загроз фізичного рівня проілюстрована можливість застосування математичної моделі. Запропонована формалізована процедура розрахунку коефіцієнтів регресії. Модель може бути використана для багаторівневого аналізу впливу можливих загроз на стан інформаційно-комунікаційних систем, визначення найбільш критичних загроз та прийняття рішень щодо створення систем захисту інформації у мережах різного призначення.

Бібл. 10, табл. 2.

Ключові слова: безпека; загрози; інформаційно-комунікаційна система; математична модель; регресійний аналіз.

Вступ. З кожним роком збільшується кількість загроз інформаційній безпеці як для корпоративних мереж, так і для окремих користувачів інтернет-послуг. В останніх річних звітах компаній Cisco [1] та Check Point Software Technologies [2] йдеться про те, що 63% всіх компаній були атаковані протягом 2015 року. Тому створення ефективних систем захисту як інформації, так і самих комп'ютерних мереж від несанкціонованого доступу та виводу з ладу інформаційних вузлів є одним з актуальних питань.

Існує велика кількість підходів до створення математичних моделей політики безпеки (Харрісона-Руззо-Ульмана (HRU), Take-Grant, Белла-ЛаПадула, Біба [3, 4]), розподілених систем захисту на основі модифікованих Е-мереж [5], прийняття рішень при проектуванні систем захисту інформації [6], обґрунтування вимог та нормування безпеки інформації в автоматизованих системах з використанням еволюційного моделювання [7], інформаційно-комунікаційних систем і мереж щодо захисту інформації на основі варіаційно-градієнтних методів [8]. Ці моделі, перш за все, спрямовані на створення теоретичної бази та орієнтовані на оцінку впливу окремих загроз на інформаційно-комунікаційні системи, аналізу стану захищеності таких систем та інформації. При вирішення практичних завдань створення систем захисту інформації у мережах різного призначення для прийняття рішення щодо використання конкретних технологій та засобів захисту і досягнення допустимого компромісу між вартістю системи захисту та її ефективністю необхідно, в першу чергу, визначити, які можливі загрози є найбільш вірогідними та критичними для конкретної мережі.

В роботі [9] запропонована багаторівнева класифікація загроз інформаційній безпеці корпоративних мереж, яка базується на таких критеріях: джерела загроз, тип впливу, переслідувані цілі, рівні моделі OSI, об'єкти та види атак. Метою даної роботи є побудова математичної моделі

загроз на основі регресійного аналізу, яка дозволить оцінити вплив можливих атак різного рівня та прийняти обґрунтоване рішення щодо реалізації системи захисту.

Теоретична модель. Регресійний аналіз використовують як ефективний інструмент визначення функції відгуку

$$Y = f(x_1, x_2, \dots x_i, \dots x_n),$$

яка встановлює аналітичний зв'язок між випадковою величиною Y – параметром оптимізації і незалежними змінними $x_1, x_2, \dots x_i, \dots x_n$ – факторами на основі експериментальних даних [10].

Метою регресійного аналізу є забезпечення максимальної точності апроксимації параметру оптимізації набором простих, частіше поліноміальних, функцій $f_i(X)$:

$$Y_{\text{mod}}(X) = \sum_{i=1}^{n} b_i f_i(X), \qquad (1)$$

де X – вектор значень вимірюваної величини; $Y_{\text{mod}}(X)$ - відгук системи, b_i – коефіцієнти поліному.

Коефіцієнти регресії b_i визначають, виходячи з критерію мінімізації суми квадратів різниці між експериментально встановленими значеннями параметра y_j і модельним значенням параметра y_{jmod} у всіх експериментальних точках j = 1, 2, 3 ... N, де N – кількість дослідів.

Для побудови моделі загроз та аналізу їх впливу на інформаційно-комунікаційні системи розглянемо задачу у наступній постановці. Визначимо матрицю X як матрицю кількісних значень можливих атак на мережу та їх комбінацій

$$X = \begin{pmatrix} 1 & x_{11} & x_{21} & . & x_{n1} & x_{11}\cdot x_{21} & x_{11}\cdot x_{31} & . & x_{n-1,1}\cdot x_{n,1} \\ 1 & x_{12} & x_{22} & . & x_{n2} & x_{12}\cdot x_{22} & x_{12}\cdot x_{32} & . & x_{n-1,2}\cdot x_{n2} \\ 1 & x_{13} & x_{23} & . & x_{n3} & x_{13}\cdot x_{23} & x_{13}\cdot x_{33} & . & x_{n-1,3}\cdot x_{n3} \\ 1 & . & . & x_{kl} & . & . & . & . & x_{n-1,l}\cdot x_{nl} \\ 1 & x_{1N} & x_{2N} & . & x_{nN} & x_{1N}\cdot x_{2N} & x_{1N}\cdot x_{3N} & . & x_{n-1,N}\cdot x_{nN} \end{pmatrix}$$

де x_{nl} - кількісне значення атаки, n – номер (вид) атаки, l – номер досліду (розглядаються як окремі атаки, так і їх можливі комбінації), матрицю Y як матрицю кількісних значень, які характеризують стан мережі (матрицю станів)

$$Y = \begin{pmatrix} y_1 \\ y_2 \\ .. \\ y_l \\ .. \\ y_N \end{pmatrix},$$

де y_l - кількісне значення стану мережі після проведення атак, матрицю B як матрицю коефіцієнтів регресії

$$B = \begin{pmatrix} b_0 \\ b_1 \\ . \\ b_n \\ . \\ b_m \end{pmatrix},$$

де n – кількість факторів, вплив яких досліджується, m – кількість членів регресійного поліному ($m < N$). Фактично m дорівнює числу стовпців матриці X.

В результаті, зв'язок між станом мережі та можливими атаками буде представлений системою рівнянь у матричному вигляді

$$(X^T X)B = X^T Y, \qquad (2)$$

де X^T – транспонована матриця X, звідки можна отримати матрицю коефіцієнтів регресії

$$B = (X^T X)^{-1} \cdot (X^T Y), \qquad (3)$$

де $(X^TX)^{-1}$ – обернена матриця (X^TX).

Множина можливих сполучень факторів X та їх значень визначає множину станів мережі Y. Теоретично кількість можливих атак на мережу та їх комбінацій може бути необмеженою, однак практично цю величину можна вважати скінченною.

Для визначення коефіцієнтів регресії та побудови аналітичної моделі загроз скористаємося наступними припущеннями [10]:

1) випадкова величина Y (параметр оптимізації) має нормальний розподіл похибки вимірювань (тобто щільність цього розподілу визначається законом Гауса). При цьому математичне сподівання та дисперсію параметру оптимізації вважають постійними величинами;

2) точність встановлення факторів набагато вища точності встановлення параметру оптимізації, тому фактори розглядають як невипадкові величини, а параметр оптимізації – випадкова величина;

3) у межах похибки визначення параметру оптимізації заданому сполученню факторів *X* повинно відповідати цілком певне значення параметру *Y*, який повинен мати фізичний зміст, область визначення і який розглядають як один з найбільш інформативних параметрів системи, що досліджують;

4) незалежні змінні *X* повинні бути сумісними, мати фізичний зміст та однозначний функціональний зв'язок з параметром оптимізації *Y*.

Усі ці припущення є коректними для задачі, що вирішується - визначення зв'язку між станами мережі та можливими атаками на неї.

В результаті, після проведення деякої обмеженої кількості дослідів, за їх результатами можна розрахувати коефіцієнти регресії та побудувати математичну модель загроз у вигляді рівняння регресії:

$$\breve{Y} = b_0 + b_1 x_1 + b_2 x_2 + ... + b_i x_i + ... + b_n x_n . (4)$$

В цій моделі під x_i розуміють як окремий фактор, так і одну з можливих комбінацій факторів. Прийнято вважати [10], що у рівнянні регресії коефіцієнт b_0 є множником фіктивного фактору $x_0 = 1$.

Рівняння (4) є апроксимаційним рівнянням, яке може бути використано для подальшого прогнозування впливу можливих атак на стан мереж різного призначення. Аналіз значень коефіцієнтів регресії дозволяє зробити висновки щодо того, які атаки несуть більшу загрозу для інформаційно-комунікаційної системи та прийняття рішень, щодо побудови системи захисту. Для заповнення матриці можливих атак *X* і матриці станів мережі *Y* можна провести аналіз статистичних даних щодо загроз та їх наслідків, скористатися експертними оцінками, результатами оціночного моделювання або експерименту.

Процедура побудови аналітичних моделей. Моделі загроз пропонується будувати з використанням їх багаторівневої класифікації [9]. Слід зауважити, що методи і технології захисту комп'ютерних мереж також реалізуються на різних рівнях, тому порівневий аналіз дозволяє прийняти обґрунтовані рішення щодо вибору технологій захисту при побудові комплексних систем захисту інформації.

Для кожного рівня необхідно вибрати найбільш розповсюджені атаки та на підставі, наприклад, експертних оцінок визначити значення можливих атак та реакцію мережі на них. В результаті буде сформована таблиця, яка міститиме результати дослідів по впливу атак на стан мережі (табл. 1).

Таблиця 1

Результати дослідів впливу атак на стан мережі

№ досліду	Атака 1	…	Атака К	Стан мережі
1	Значення 1і		Значення Кі	Значення m
…..				
N	Значення 1і		Значення Кі	Значення m

де *N* – кількість дослідів, *к* = 1 … *K* - різновиди атак, *i* = 1 … *I* – кількісне значення можливого варіанта атаки (для кожної атаки верхня границя *I* буде відрізнятися), *m* = 0 … *M* - кількісний показник реакції мережі на комбінацію атак.

Виходячи зі структури мережі, спеціалізації роботи компанії, вірогідності проведення конкретної атаки на підставі аналізу статистичних даних, експертних оцінок, результатів оціночного моделювання або експерименту атакам присвоюються імовірнісні коефіцієнти *Vk* = 0 … 1 (*к* = 1 …*K*), які характеризують стабільність стану мережі на проведення атаки (чим більше коефіцієнт, тим більше імовірність стабільної роботи мережі). Перемноживши присвоєні коефіцієнти на кількісні значення атак (табл. 1) отримаємо матрицю атак *X* (табл. 2). Далі, використовуючи рівняння (3) розраховуємо коефіцієнти регресії b_i, що дозволить нам отримати аналітичну модель загроз у вигляді рівняння регресії (4). Аналіз значень коефіцієнтів регресії дозволить відсіяти найменш критичні атаки та прийняти обґрунтоване рішення щодо вибору технологій та засобів захисту для реалізації системи захисту мережі.

Для практичного застосування запропонованого математичного апарату, збільшення універсальності та адекватності аналітичних моделей необхідне формування бази даних атак і їх впливу на мережі різного призначення та проведення достовірних експертних оцінок для визначення вагових коефіцієнтів. Це є окремою задачею, вирішення якої виходить за рамки даної статті і потребує подальших досліджень.

Таблиця 2

Матриця атак з присвоєними ймовірностями

№ досліду	Атака 1	…	Атака К	Стан мережі
1	V1 * Значення 1і		VК * Значення Кі	Значення *m*
…..				
N	V1 * Значення 1і		VК * Значення Кі	Значення *m*

Висновки. Засобами регресійного аналізу розроблено математичний апарат, який може бути використаний для обробки даних, отриманих з різних джерел (аналітичних звітів, експериментальних досліджень або модельних експериментів над конкретними мережами, експертних оцінок, тощо) і побудови апроксимаційних аналітичних моделей, які дозволять оцінити вплив можливих атак різного рівня на інформаційно-комунікаційні системи та прийняти обґрунтоване рішення щодо реалізації системи захисту. Для розрахунку коефіцієнтів регресії розроблена формалізована процедура. Процедуру пропонується використовувати для кожного рівня моделі OSI, що дозволить отримати аналітичні моделі загроз відповідного рівня. При побудові моделі загроз для конкретної мережі необхідно враховувати особливості структури мережі, спеціалізації роботи компанії, вірогідність проведення конкретної атаки. Кількісні значення факторів, що використовуються для побудови моделі можуть бути отримані на підставі аналізу статистичних даних, експертних оцінок, результатів оціночного моделювання або експерименту. Формуючи базу даних атак та результатів дослідів їх впливу на стан інформаційно-комунікаційних систем, можна збільшити універсальність моделі та її адекватність, що дозволить застосовувати її до систем різного призначення з різними вимогами до інформаційної безпеки.

Надійшла до редакції 02 березня 2017 р.

УДК 004.056, 004.75
Кучернюк П. В., к.т.н., OrcID 0000-0001-6381-0156
e-mail kuchernuk@kpi.ua
Национальний технический університет Украины
«Киевский политехнический институт имени Игоря Сикорского»
Довгаль А. А., OrcID 0000-0002-4035-110X
e-mail dovgal.andrey@ua.sika.com
компания «Сика»

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ РЕГРЕССИОННОГО АНАЛИЗА

Средствами регрессионного анализа с использованием многоуровневой классификации угроз, которая базируется на модели OSI, разработана математическая модель угроз безопасности в информационно-коммуникационных системах. Рассмотрена постановка задачи и показано, как из теоретической модели получить аппроксимационное уравнение регрессии, которое может быть использовано для дальнейшего прогнозирования влияния возможных атак на состояние сети. Предложена формализованная процедура расчета коэффициентов регрессии и на примере угроз физического уровня проиллюстрирована возможность использования математической модели. Модель может быть применена для многоуровневого анализа влияния вероятных угроз на состояние информационно-коммуникационных систем, определения наиболее критичных угроз и принятия решений по созданию систем защиты информации в сетях различного назначения.

Библ. 10, табл. 2.

Ключевые слова: *безопасность; угрозы; информационно-коммуникационная система; математическая модель; регрессионный анализ.*

UDC 004.056, 004.75
P. V. Kucherniuk, PhD, OrcID 0000-0001-6381-0156
e-mail kuchernuk@kpi.ua
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
A. O. Dovhal, OrcID 0000-0002-4035-110X
e-mail dovgal.andrey@ua.sika.com
Sika Ukraina

MODEL THREATS TO SECURITY OF INFORMATION AND COMMUNICATIONS SYSTEMS BASED ON REGRESSION ANALYSIS

Mathematical model of threats to security of information and communication systems was developed by means of regression analysis to determine, which potential threats are most probable and critical for a particular network and to decide in the further on the use of specific technologies and means of protection. The multilevel classification of threats which based on the OSI model and takes into account such criteria as the source of the threats, the type of impact, objectives pursued, objects and types of attacks was used in constructing the model. The statement of the problem of regression analysis was considered and was showed as from theoretical model get the approximation regression equation which can be used to further forecasting the impact of possible attacks on the network state. Statistics on threats and their consequences, expert assessments, the results of the evaluation simulation or experiment are proposed to use to fill a matrix of possible attacks and network states. For calculating the regression coefficients for approximating analytic model as a regression equation the formalized procedure was proposed. This procedure is proposed to use for each OSI model level, which will provide analytical model appropriate level threats. The model can be used for multilevel analysis of the impact of possible threats to the state of information and communication systems, identifying the most critical threats and making decisions on creation of information security systems in networks for different purposes. The versatility of the model and its adequacy can increase by creating a database of attack and experimental results of their impact on the information and communication systems. This will apply the model to systems for various purposes with different requirements for information security.

References 10, Tables 2.

Keywords: *security; threats; information and communication system; mathematical model; regression analysis.*

References:

[1]. "Cisco Annual Report on Information Security for 2016," 2016. [Online]. Available: http://www.cisco.com/c/m/ru_ru/offers/sc04/2016-annual-security-report.

[2]. "2016 Security Report," Check Point Software Technologies Ltd., [Online]. Available: http://www.secdatacom.dk/files/agenturer/check%20point/2016-security-report.pdf.

[3]. Graivoronsky, M. V.; Novikov, O. M., Bezpeka informatsiino-komunikatsiinyh system [Information and communication systems security], Kyiv: Publishing Group BHV, 2009, p. 608.

[4]. Dudykevich, V. B.; Opirsky, I. R., «AnalIz modeley zahistu InformatsIYi v InformatsIynih merezhah derzhavi [Analysis of models of information security in information networks of state],» *Information processing systems,* № 4, pp. 86-89, 2016, **URL:** http://nbuv.gov.ua/UJRN/soi_2016_4_18

[5]. E. N. Davydova, «Matematicheskoe modelirovanie raspredelennyih sistem zaschityi informatsii [Mathematical modelling of the distributed systems of security of the information],» *Programmnye produkty i sistemy,* № 2, pp. 57 - 61, 11 06 2011,
URL: http://www.swsys.ru/index.php?page=article&id=2764

[6]. Pavlov, I. N.; Tolyupa, S. V., «AnalIz pIdhodIv otsInki efektivnostI matematichnih modeley pri proektuvannI sistem zahistu InformatsIi,» *Modern information security,* № 3, pp. 36-44, 2014,
URL: http://nbuv.gov.ua/UJRN/szi_2014_3_9

[7]. Khvostov, V. V.; Rogozin, E. A.; Nikulina, E. Y., «Obosnovanie norm bezopasnosti informatsii avtomatizirovannyih sistem s ispolzovaniem metodov evolyutsionnogo modelirovaniya [Justification Safety standards of automated information systems with the use of evolutionary modeling methods],» *The bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia,* № 4, pp.

197-203, 2014,
URL: https://ви.мвд.рф/Nauka/nauchnij-zhurnal-vestnik/Vestnik_arhiv/item/6897080/

[8]. Khoroshko, V. A.; Maysak, T. V.; Dakhno, N. B., «Matematichni modeli informatsiino-komunikatsiinyh sistem i merezh schodo zahistu informatsii na osnovi teorii variatsiino-gradiientnyh metodiv [Mathematical models of information and communication systems and networks to protect information based on the theory of variational-gradient methods],» *Modeling and Information Systems in the economy,* № 91, pp. 246 - 255, 2015,
URL: http://nbuv.gov.ua/UJRN/Mise_2015_91_25

[9]. A. O. Dovhal, «KlasifIkatsIi zagroz bezpeki v InformatsIynIy merezhI [Classification of security threats in the information network],» в *IX Interna-tional Scientific Conference of Young Scientists "Electronics-2016". Collection of articles*, Kyiv, 2016, **URL:** http://elconf.kpi.ua/wp-content/uploads/2016/04/ELCONF-2016_sbornik.pdf

[10]. P. Yahanov, Regresiinyi analiz bagatofaktornyh tehnichnyh system. Teksty lektsii dlia vyvchennia rozdiliv distsiplini "Osnovy naukovo-doslidnoii produktsii" [Regression analysis of multifactor technical systems. Texts of lectures to study sections of discipline "Fundamentals of research production"], Kyiv: PPC VPI "Polytechnic", 2006, p. 36.