Challenges and threats to critical infrastructure. Collective monograph - NGO Institute for Cyberspace Research (Detroit, Michigan, USA), 2023. - 325 p.

The collective monograph was prepared by ukranian scholars within the framework of studies of a wide range of security issues. The authors of the monograph look at the problems of security of the state`s security in a rich manner behind such basic warehouses as military security, information security, military-technical security, environmental and technogenic security

Reviewers:

Ponomarev S.P. - Doctor of Jurisprudence, head of the Department of Administration of the State Service of Special Communications and Information Protection of Ukraine

Hnatyuk S.O. - Ph.D. Chief Researcher of the State Scientific and Research Institute of Cybersecurity Technologies and Information Protection

Silvestrov A.M. - Ph.D. Prof. National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”


**ISBN-10/979-8-218-22315-1**

**Authors**

**Chapter 1.** Avramenko O.V., Polishchuk V.V., Sarapin Yu.O., Voinov I.A. 1, V.A. Malik, N.V. Zhenyuk, N.I. Voropai, O.G. Korol, A.Yu. Strelnikova, Yu.V. Kostenko, O.V. Peredrii, V.V. Gordiychuk, Grinenko O.I., Hrytsyuk V.V., Zubkov V.P., Ptashkin R.L., Palagin V.V., Savostyanenko M.V., Klymenko K.V., Klymenko K.V., Tyutyunyk V . ., Kapelushna T.V.

**Chapter 2.** Azarenko O., Honcharenko Yu., Divizinyuk M., Shevchenko R., Shevchenko O., V.M. Vashchenko, V.I. Skalozubov, I.B. Korduba, Shcherbak O., Khmyrova A., Khrystych V., Zhuk V. M., Pohosyan G. A., Yevlanov M. V., Cherepnyov I. A., Chumachenko S. M., Kolomiets D. P., Matsko P. I., Kaplia I. O., Romanyuk V. P., Medvedev M. G., Mulyava O. M., Peredrii O. V., Komisarov M. V., Proshchyn I. V., Sydorenko V .L., Eremenko S.A., Tyshchenko V.O., Vlasenko E.A., Pruskyi A.V., Demkiv A.M., Yudina D.O.

**Chapter 3.** V. N. Yelisieiev, E. V. Bykova, V. S. Tyshchenko, N. V. Zaika, V. A. Popel, S. S. Chumachenko, O. V. Ivchenko, V. V. Palagin, R. Kyrychok. V., Laptev O.A., Laptev S.O., Sobchuk A.V., Ponomarenko V.V., Barabash A.O., Murasov R.K., Chumachenko S.M., Sirik A.O. , Yevtushenko O.V., Sobchuk V.V., Pichkur V.V., Lapteva T.O., Kopytko S.B.

**Chapter 4.** Goncharenko I.O., Kuchma T.L., Prodanyuk D.M., Zaretskyi I.S., Karpenko M.I., Moshenskyi A.O., Derman V.A., Khoperskyi S. V., Chumachenko S.M., Ponomarenko S.O., Popel V.A, Maslennikova T.A.

**Chapter 5.** Vovchuk T., Shevchenko R., Shevchenko O., Guida O.G., Kiselyov V.B., Ometsynska N.V., Trysnyuk T.V., Konetska O.O., Nagornyi E. I., Marushchak V.M., Volynets T.V., Prystupa V.V., Trofimchuk O.M., Trysnyuk V.M., Shumeiko V.O., Chumachenko S.M., Lysenko O.I. , O. M. Tachynina, O. V. Furtat, S. O. Furtat, I. O. Sushin.

**Chapter 6.** Viola Vambol, Alina Kowalczyk-Juśko, Sergij Vambol, Nadeem Ahmad Khan, Aaron Dumont, Zaporozhchenko M.M., Legominova S.V., Muzhanova T.M., Ometsynska N.V., Kiselyov V. B., Huida O. G., Shchavinskyi Y.V., Palchynska V.B.

**Chapter 7.** Altaf Hussain Lahori, Barbara Savytska, Parisa Ziarati, Barbara Krokhmal-Marchak, Niloofar Mozaffari, Nastaran Mozaffari, Miasoyedova A., Divizinyuk M., Shevchenko R., Myroshnychenko A., Aldoshin O.O., Kalinovsky A.Ya., Vykhvatin M.V., Havrys A.P., R.S. Yakovchuk, O.O. Pekarska, M.V. Yevlanov, R.V. Antoshchenkov, I.A. Cherepnyov, I.I. Kravchenko, V. Loik. B., Synelnikov O.D., Goncharenko M.O., Nazarenko S.Yu., Mandrychenko D.S., Shapovalov M.M., Pichugin M.A., Vynogradov S.A., Samchenko T.V. , Nuyanzin O.V., Sverchkov O.V., Faure E.V., Skutskyi A.B., Lavdanskyi A.O., Grechanyk O.S., Shakhov S.M., Zinchenko O.O., Yatsenko V.O., Vambol S.O.

**Chapter 8.** Adamova G.V., Anila Kausar, Ambreen Afza, Altaf Hussain Lahori, Bobkov Y.V., Shevchuk A.A., Stamati V.G., Vynogradov S.A., Chumachenko S.M., Lysenko O.I., Novikov V.I., Furtat O.V., Furtat S.O., Sushin I.O., Pisnya L.A., Mishchenko I.V., Vambol S.O., Vambol Viola

**Chapter 9.** Yakovliev Ye.O., Rudko G.I., Yermakov V.M., Chumachenko S.M., Kodryk A.I., Dyatel O.O., Lubenska N.O.

## *CONTENT*

УДК 004.056

# 29.МЕТОДОЛОГІЯ ПІДТВЕРДЖЕННЯ МОЖЛИВОСТІ РЕАЛІЗАЦІЇ ВИЯВЛЕНИХ ВРАЗЛИВОСТЕЙ В КОРПОРАТИВНІЙ МЕРЕЖІ З ВИКОРИСТАННЯМ ПОЛІНОМІАЛЬНИХ ПЕРЕТВОРЕНЬ БЕРНШТЕЙНА

**Киричок Р.В.[1], Лаптєв О.А.[2]**

*1 Київський університет імені Бориса Грінченка, Київ, Україна*
*2 Київський національний університет імені Тараса Шевченка, Київ, Україна*
*E-mail: r.kyrychok@kubg.edu.ua, alaptev64@ukr.net*

# METHODOLOGY FOR CONFIRMING THE FEASIBILITY OF EXPLOITING DETECTED VULNERABILITIES IN A CORPORATE NETWORK USING POLYNOMIAL TRANSFORMATIONS OF BERNSTEIN

*This report presents the results of an experimental study of the modern vulnerability exploitation tools functioning. Based on this, general quantitative characteristics of the vulnerability validation process were identified, including the number of successfully and unsuccessfully validated vulnerabilities. To describe the dynamics of this process, taking into account the complex and changing nature of the environment, a mathematical model of the analysis of these characteristics based on Bernstein polynomials was developed. In particular, the proposed model allows to obtain analytical dependencies for the aforementioned characteristics, which in turn makes it possible to build probability distribution laws for them and predict the next values of their magnitudes.*

Червень 2017 року – вірус NotPetya атакував інфраструктуру великих компаній, таких як Нова пошта, Нафтогаз, Київенерго, а також інфраструктуру багатьох банків та мобільних операторів.

Грудень 2020 року – в ході спланованої кібероперації було заражене комп'ютерним вірусом програмне забезпечення SolarWinds, яке використовують державні служби та великі корпорації багатьох країн світу.

Це лише пару прикладів найбільш гучних інцидентів кібернетичної безпеки, які призвели до значних фінансових, репутаційних збитків, а також погіршення життєзабезпечення населення відповідної країни на певний період часу, через основні цілі даних кібероперацій, серед яких, значна частина є об'єктами критичної інфраструктури. Щодня кількість об'єктів критичної інфраструктури, які атакують зловмисники, зростає. Особливо це стало актуальним під час пандемії, коли бізнес-процеси перейшли в онлайн-формат, що ще більше привернуло увагу кіберзлочинців. Згідно зі звітом ENISA [1], Агентства Європейського Союзу з кібербезпеки, в 2020-2021 роках зросла кількість атак на так звані «домашні офіси», тобто програмне забезпечення, що дозволяє створювати єдину корпоративну мережу та особисті кабінети працівників задля дистанційної форми праці. Це призвело до збільшення загрози витоку даних для бізнесу з 8,7% у 2020 році до 81% у другому кварталі 2021 року.

Крім того, компанія Accenture зафіксувала у своєму звіті [2] від листопада 2021 року, що 55% компаній (з річним доходом більше 1 млрд. доларів) недостатньо ефективно попереджають кібератаки, надто повільно виявляють та усувають уразливості.

Така тенденція зокрема стала можливою через відносну тривіальність подолання мережевого периметру, оскільки більшість атак носить рутинний характер, а їхня реалізація все ще залишається можливою лише через те, що компанії не здійснюють своєчасне оновлення свого програмного забезпечення, в результаті чого, відомі вразливості роками залишаються «незакритими». Водночас така ситуація ускладнюється динамічним зростанням кількості вразливостей та їх критичності [3], на ряду зі спрощенням проведення атак за рахунок вже готових експлойтів (програмних модулів, що використовують слабкі місця в компонентах інформаційно-комунікаційних систем та вразливості в ПЗ з метою реалізації несанкціонованого впливу на цільову систему, проведення атаки), які можна знайти у відкритих базах, або просто придбати, найчастіше в даркнеті.

За таких умов, для забезпечення безпеки інформаційних систем, важливим напрямком є впровадження превентивних механізмів. Серед таких механізмів, досить перспективними виявляються методи активного аналізу захищеності, оскільки вони дозволяють виявити та підтвердити можливість реалізації конкретних вразливостей. Це, в свою чергу, дозволяє визначити фактичний рівень безпеки інформаційних систем та мереж, на основі чого, вже формувати рекомендації щодо усунення підтверджених вразливостей.

Тому удосконалення технологій своєчасного виявлення та закриття вразливостей у корпоративних мережах, що дозволяють мінімізувати ризик проведення кібератаки, є актуальним питанням.

Отже, виходячи з вищезазначеного, було проведено експериментальне дослідження функціональних можливостей сучасних автоматизованих засобів експлуатації вразливостей в ході якого виявлено, що якість перевірки та підтвердження можливості реалізації вразливостей цільових об’єктів корпоративного мережного оточення можна представити у вигляді вектора $(q_s, q_f, q_c)$ трьохвимірного векторного простору, де $q_s$ – абсциса, яка визначає кількість успішно перевірених вразливостей, $q_f$ – ордината, яка визначає кількість неперевірених вразливостей та $q_c$ – аппліката, яка визначає кількість випадків перевірки вразливостей, що призвели до критичних помилок на цільовому об’єкті та подальшої втрати з ним зв’язку.

В результаті, було побудовано математичну модель аналізу кількісних характеристик процесу підтвердження можливості реалізації вразливостей інформаційних систем методом регресійного аналізу. Для цього, спершу оцінюючи статистичний зв’язок між змінними $t$ і $q_s$, $q_f$, $q_c$ з використанням коефіцієнта кореляції $R$, встановлено його лінійність.

При цьому слід зазначити, що найтісніший лінійний зв’язок спостерігався між значеннями $t$ та $q_f$ . Відповідно, можна стверджувати, що при збільшенні одного значення в середньому збільшується й інше.

Задля подання емпіричних залежностей між параметрами, що описують поведінку процесу підтвердження можливості реалізації вразливостей інформаційних систем в зрозумілій та стислій формі, було прийнято рішення апроксимувати експериментальні дані. Водночас, задля отримання найбільш достовірних коефіцієнтів апроксиманти, скористалися теоремою Бернштейна [4, 5].

Дана теорема полягає в тому, що довільну неперервну функцію *f(t)*, яка визначена і неперервно-диференційована на відрізку [0;1], можна представити у вигляді поліному:

$$B_n(f;t_н) = B_n(t_н) = \sum_{k=0}^{n} f\left(\frac{k}{n}\right) b_{k,n}(t_н), \tag{1}$$

де $b_{k,n}(t_н) = C_n^k t_н^{\,k}(1-t_н)^{n-k}$, $C_n^k = \dfrac{n!}{k!(n-k)!}$, $t_н$ – нормований час.

Виходячи з результатів проведеного експериментального дослідження, було встановлено, що час раціонального циклу перевірки вразливостей у випадку інструменту *Armitage* становить 345 секунд. Тому, спершу, слід нормувати часовий інтервал наступним чином:

$$t_н = \frac{t_i}{T} \tag{2}$$

де $T$ – час перевірки вразливостей цільового об'єкта корпоративного мережного оточення за секунди (час раціонального циклу);

$t_i$ – час, протягом якого відповідні характеристики $(q_s, q_f, q_c)$ приймали свої значення в рамках раціонального циклу.

Після чого, наступним кроком, використовуючи отримані статистичні дані, розрахований нормований час $t_н$ та вираз (1), отримуємо початкові аналітичні залежності для кожної з характеристик. Так, до прикладу, для кількості успішно перевірених вразливостей $q_s=q_s(t_н)$ було отримано наступні початкові аналітичні залежності:

$$\begin{aligned} q_s(t_н) = {} & q_s(0)b_{0.11}(t_н) + q_s(0{,}168)b_{1.11}(t_н) + q_s(0{,}188)b_{2.11}(t_н) + q_s(0{,}206)b_{3.11}(t_н) + \\ & + q_s(0{,}238)b_{4.11}(t_н) + q_s(0{,}241)b_{5.11}(t_н) + q_s(0{,}249)b_{6.11}(t_н) + q_s(0{,}333)b_{7.11}(t_н) + \\ & + q_s(0{,}446)b_{8.11}(t_н) + q_s(0{,}849)b_{9.11}(t_н) + q_s(0{,}957)b_{10.11}(t_н) + q_s(1)b_{11.11}(t_н). \end{aligned}$$

Останнім кроком здійснюємо підстановку відповідних поліномів $b_{k,n}(t_н)$ та вираховуємо безпосередньо самі значення даних аналітичних залежностей:

$$\begin{aligned} q_s(t_н) = {} & b_{1.11}(t_н) + 2b_{2.11}(t_н) + 2b_{4.11}(t_н) + b_{5.11}(t_н) + 3b_{6.11}(t_н) + b_{7.11}(t_н) + \\ & + 3b_{9.11}(t_н) + 3b_{10.11}(t_н) + 3b_{11.11}(t_н). \end{aligned} \tag{3}$$

Аналогічним чином були отримані початкові аналітичні залежності для кількості неперевірених вразливостей $q_f=q_f(t_н)$, (4) та кількість випадків перевірки вразливостей, що призвели до критичних помилок $q_c=q_c(t_н)$, (5):

$$q_f(t_н) = 81b_{1.11}(t_н) + 80b_{2.11}(t_н) + 39b_{3.11}(t_н) + 92b_{4.11}(t_н) +$$
$$+45b_{5.11}(t_н) + 93b_{6.11}(t_н) + 61b_{7.11}(t_н) + 83b_{8.11}(t_н) +$$
$$+762b_{9.11}(t_н) + 777b_{10.11}(t_н) + 306b_{11.11}(t_н). \quad (4)$$
$$q_c(t_н) = b_{1.11}(t_н) + 3b_{2.11}(t_н) + 2b_{4.11}(t_н) +$$
$$+2b_{6.11}(t_н) + b_{7.11}(t_н) + b_{8.11}(t_н) + 3b_{11.11}(t_н). \quad (5)$$

Таким чином, в результаті було отримано наступні аналітичні залежності:

$$q_s(t_н) = \sum_{i=0}^{n} q_s(t_н^{(i)}) b_{k,n}(t_н),$$
$$q_f(t_н) = \sum_{i=0}^{n} q_f(t_н^{(i)}) b_{k,n}(t_н),$$
$$q_c(t_н) = \sum_{i=0}^{n} q_c(t_н^{(i)}) b_{k,n}(t_н).$$

які є остаточними виразами для досліджуваних характеристик процесу перевірки та підтвердження можливості реалізації вразливостей інформаційних систем.

**Висновки**

1. У ході експериментального дослідження функціонування сучасних засобів експлуатації вразливостей було виявлено узагальнені характеристики процесу перевірки вразливостей.

2. Розроблено математичну модель для аналізу кількісних характеристик процесу перевірки вразливостей з урахуванням складного та мінливого характеру середовища. Особливістю розробленої моделі є застосування поліноміальних перетворень Бернштейна.

3. У ході моделювання аналізу узагальнених кількісних характеристик процесу перевірки вразливостей було виведено їх аналітичні залежності, що повною мірою відображають динаміку цього процесу.

**Література**

1. ENISA Threat Landscape 2021 (European union agency for cybersecurity) [Електронний ресурс] – Режим доступу до ресурсу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

2. State of Cybersecurity Resilience 2021 (4th Annual Report): How aligning security and the business creates cyber resilience. Accenture. [Електронний ресурс] – Режим доступу до ресурсу: https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf

3. CVSS Severity Distribution Over Time [Електронний ресурс] – Режим доступу: https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time.

4. Approximation and Interpolation, by Philip J. Davis (Dover Publications, 1975), ISBN 3-486-62495-1. Originally published in 1963. "while [Bernstein's proof] is not the simplest conceptually", p. 108.

5. Bernstein Polynomials, by G. G. Lorentz (Chelsea Publishing Company, 1986), ISBN 978-0-8218-7558-2. Originally published in 1953.

УДК 004.056.53

# 30.ПАРАМЕТРИЧНИЙ МЕТОД СПЕКТРАЛЬНОГО АНАЛІЗУ СИГНАЛІВ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

**Лаптєв С.О.[1], Собчук А.В.[2], Пономаренко В.В.[2], Барабаш А.О.[3]**
*[1] Київський національний університет імені Тараса Шевченка, м. Київ, Україна*
*[2] Державний університет телекомунікацій, м. Київ Україна*
*[3] Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ Україна*
*e-mail:* salaptiev@gmail.com, anri.sobchuk@gmail.com, Ur_suviator @ukr.net, andrew.barbsh@gmail.com

## Parametric method of spectral analysis of signals of critical infrastructure objects

*The research established that the method of spectral analysis, based on the classical Prony method, improved by replacing fading sinusoids with the use of non-fading sinusoids, allows you to very accurately isolate the signal and determine its characteristics in a space rich in interference. The method will be useful for tracking unauthorized access to information systems of critical infrastructure facilities. In order to confirm the chosen method of spectral analysis, simulations were carried out and graphs of spectrograms of the pulse signal were obtained using Fourier, Chebyshev, and Bessel methods. The obtained graphical data fully confirm the advantages of our proposed method for the spectral analysis of random short-term pulses*

Проблематика моніторингу сигналів пристроїв несанкціонованого доступу до інформаційних систем об'єктів критичної інфраструктури залишається однією з найгостріших проблем сьогодення [1]. Стрімкий розвиток інформаційних технологій вимагає постійного вдосконалення методів моніторингу. Необхідно зазначити, що останнім часом зріс інтерес до параметричних методів спектрального аналізу. Методи спектрального аналізу випадкових сигналів діляться на два великі класи – непараметричні і параметричні. У непараметричних методах використовується тільки інформація, що міститься у даних аналізованого сигналу. Параметричні методи передбачають наявність деякої статистичної моделі випадкового сигналу, а процес спектрального аналізу в даному випадку містити визначення параметрів цієї моделі [2].

Значна роль в аналізі сигналів належить комплексному перетворенню Фур'є [3]. Перетворення Фур'є (ПФ) і його дискретні аналоги (ДПФ) добре відомі та широко застосовуються в техніці спектрального аналізу при стандартній