DOI: https://doi.org/10.32782/2524-0072/2023-51-27

УДК 330.43:330.46

ПРОГНОЗУВАННЯ ІНФОРМАЦІЙНИХ ТРЕНДІВ КІБЕРАТАК ЯК ІНСТРУМЕНТ ПРОТИДІЇ ВРАЗЛИВОСТЕЙ В ЕКОНОМІЦІ[1]

FORECASTING INFORMATION TRENDS CYBERATTACKS AS A TOOL FOR COUNTERING VULNERABILITIES IN THE ECONOMY

Яровенко Ганна Миколаївна
докторка економічних наук, доцентка,
Сумський державний університет;
запрошена професорка,
Мадридський університет Карлоса III
ORCID: https://orcid.org/0000-0002-8760-6835

Солярова Катерина Геннадіївна
бакалаврантка,
Сумський державний університет
ORCID: https://orcid.org/0009-0001-5960-6993

Yarovenko Hanna
Sumy State University;
University Carlos III of Madrid

Soliarova Kateryna
Sumy State University

Дана стаття присвячена питанню прогнозування інформаційних трендів кібератак за допомогою побудови авторегресійних моделей. Розрахунки проводилися на основі даних Google Trends для соціальної інженерії, DoS-атак та атак на паролі користувачів за період з 28.01.2018 по 22.01.2023. Проведений тест Харке-Бера та аналіз гістограм розподілу встановили необхідність логарифмування даних соціальної інженерії та атак на паролі користувачів. Розширений тест Дики-Фулера підтвердив стаціонарність рядів соціальної інженерії та DoS-атак. Декомпозиція трендів виявила наявність сезонної компоненти для соціальної інженерії та атак на паролі користувачів. В результаті для DoS-атак побудовано ARMA-модель, для інших рядів – SARIMA із сезонною та авторегресійною компонентами. Тести верифікації залишків та прогнозів виявили задовільною модель для DoS-атак, соціальної інженерії – високого рівня, хоча із наявною автокореляцією залишків для сезонного лагу, для атак на паролів користувачів – високого рівня, але із наявною гетероскедастичністю залишків.

Ключові слова: ARIMA-модель, вразливість, економіка, кібератака, прогнозування, SARIMA-модель.

This article is devoted to the issue of forecasting information trends of cyberattacks using the construction of autoregression models. The study's results will contribute to forming a strategy for countering cybercrimes at the macro level, reducing the impact of their negative consequences on development and the emergence of vulnerabilities in economic processes. Calculations were made based on Google Trends data for three types of cyber attacks related to social engineering, DoS attacks and attacks on user passwords. The data set was created from January 28, 2018, to January 22, 2023. Calculations were performed using the Python programming language. The process of forecasting consisted of the implementation of several preliminary tests, the construction of forecast models and their verification. Conducted Jarque–Bera test and analysis of distribution histograms for each data series established the necessity of logarithmizing the series of social engineering and attacks on user passwords. The extended Dickey–Fuller test confirmed the stationarity of the social engineering and DoS attacks. The time series of attacks on user passwords is non-stationary, so it will be integrated with the simulation process. The decomposition of trends revealed the presence of a seasonal component for social engineering and attacks on user passwords with lag 52.

[1] Робота виконана в рамках держбюджетної науково-дослідної роботи 0121U109559 «Національна безпека через конвергенцію систем фінансового моніторингу та кібербезпеки: інтелектуальне моделювання механізмів регулювання фінансового ринку»

© Яровенко Г.М., Солярова К.Г. 2023

As a result, an ARMA model with autoregression and moving average components was built for DoS attacks, and SARIMA with seasonal and autoregressive elements for other series. The models were constructed iteratively based on analysing AIC, BIC and HQIC information criteria. As a result, those with the best values were selected. The residuals and forecast verification tests revealed a satisfactory model for DoS-attacks, social engineering – high level, although with the presence of autocorrelation of the residuals due to the seasonal component, for attacks on user passwords – high level, but with the presence of heteroscedasticity of the residuals, which requires further modification of the model. Although the prediction results turned out to be ambiguous, the constructed models can be used to predict cybercrimes related to DoS attacks and social engineering.

Keywords: ARIMA model, vulnerability, economy, cyber attack, forecasting, SARIMA model.

Постановка проблеми. За останнє десятиріччя спостерігається зростання кібератак в різних сферах життєдіяльності суспільства. Мета їх здійснення є різною, починаючи від незаконного присвоювання персональних даних та завершуючи порушенням функціонування діяльності низки підприємств. Від кіберзлочинів страждають енергетичні системи, системи управління технологічними процесами, різні об'єкти інфраструктури, компанії різних секторів бізнесу, фінансові організації, фізичні особи – Інтернет-користувачі та користувачі різних мобільних та програмних додатків, тощо.

Можна навести багато прикладів, коли в результаті кібератак було нанесено значну шкоду, яка обернулася багатомільйонними збитками. Наприклад, у 2016 році кіберзлочинці намагалися викрасти 1 млрд дол. із золотовалютних резервів Бангладешу, унаслідок чого країна втратила 101 млн дол. Хакерське угрупування «The Shadow Brokers» виконало успішний злам інформаційних систем у серпні 2016 року, в результаті якого було виставлено на аукціон викрадену інформацію з початковою ставкою 1 млн. біткоїнів. Здійснення фішингової кібератаки на університети та компанії США у березні 2018 року призвело до викрадення персональної інформації вартістю 3,4 млрд дол. У грудні 2020 року постраждали 18000 державних та недержавних установ в США від масової кібератаки.

Наведені приклади є тільки невеликим свідченням щодо масштабності проблеми кіберзлочинів, вчинених проти різних суб'єктів економіки, та її наслідків, на подолання яких витрачаються фінансові ресурси постраждалих. Слід зазначити, що кошти, отримані від кіберзлочинів, є одним із джерел формування тіньового сектору економіки, оскільки їх отримання є незаконним та відповідно не пов'язано зі сплатою державних податків чи зборів. Також вони можуть спрямовуватися на розвиток, наприклад, Даркнету, закупівлю зброї, фінансування терористичних актів, підтримки наркотрафіку та інших злочинних видів діяльності. Все це створює певні вразливості у розвитку економіки, які гальмують формування економічних відносин між різними суб'єктами економіки. Саме тому дуже важливо досліджувати інформацію щодо масових кібератак та створювати прогнози щодо потенційних кіберзлочинів. Це сприятиме розробці відповідних стратегій кіберзахисту та протидіяти потенційним загрозам як на рівні окремого суб'єкта господарювання, так й на рівні країни в цілому.

Аналіз останніх досліджень і публікацій. Проблема впливу кібератак на різні сфери економіки є специфічною для вирішення у наукових колах, оскільки більшість досліджень спрямовані на розробку заходів їх виявлення та протидії на програмному та технічному рівні. Але слід відмітити, що вона набуває також актуальності й у різних аспектах, пов'язаних із розвитком економіки країн. Так, Кокаджі А. та Гото А. запропонували модель витрат і результатів для оцінки економічних втрат, спричинених кібератаками, та її використання на національному рівні [1]. Тіан С., Чжао Б. та Оліварес Р. О. досліджували вплив нових типів кіберризиків на настрої центральних банків з урахуванням їх взаємодії із приватним сектором та фінансовою системою [2]. Клампс П. оцінив механізми управління кіберризиками для страхових компаній Великобританії у контексті впливу на ці процеси з боку регуляторних органів [3]. Гейманн Ф., Генрі С. та Галус М. проаналізували електроенергетичний сектор Швейцарії на предмет рівня зрілості його кіберзахисту та запропонували рекомендації щодо його покращення [4]. Гафні Р. та Павел Т. Спрямували своє дослідження на виявлення змін у кібератаках на сектор охорони здоров'я у період глобальної пандемії COVID-19 [5]. Кірімхан Д. надав пропозиції щодо формування заходів боротьби із відмиванням грошей, отриманих злочинним шляхом, оскільки такі операції є найбільш вразливими для масових кібератак, або можуть бути пов'язаними із кіберзлочинною діяльністю [6].

Параскева А. Обгрунтувала стратегії кібербезпеки для сектору подорожей та туризму [7]. Пунт Е., Монштадт Дж., Френк С. та Вітте П., одними із перших приділили увагу проблемі кібератак на морські порти та запропонували стратегію їх дій у випадку очікування збоїв, які можуть бути викликані в результаті кіберзлочину [8]. Балікер Ч., База М., Алурані А., Альшехрі А., Альшахрані Х. та Чу К. Р. розробили пропозиції щодо створення відповідних інструментів протидії кіберзагрозам у FinTech галузі, які базуються на блокчейн-технології [9]. Фан С. та Янг З. присвятили своє дослідження чутливості транспортної системи до різного роду кіберризиків та запропонували концептуальну основу для здійснення спільного аналізу її безпеки [10]. Санчес М.А. та Де Батіста М. дослідили, які збої можуть бути в компаніях в результаті кіберхакерських атак та які макро- і мікрофактори також можуть впливати на формування вразливостей у їх діяльності [11]. Крозіньяні М., Макіавеллі М. та Сільва А.Ф. проаналізували ті наслідки, які мають компанії в результаті порушення ланцюгів постачань внаслідок здійснення масових кібератак [12].

Таким чином, наукова спільнота присвячує значну увагу проблемі кіберзлочинів та кіберзахисту для різних сфер економіки та здійснює аналітичні огляди, пропонує різні стратегії. З іншого боку, не достатньо уваги приділяється прогнозним методам, які дозволяють передбачати потенційні загрози та швидко реагувати на них. Особливо це є актуальним на макроекономічному рівні, оскільки є потреба у виявленні певних вразливостей, які можуть бути, як джерелом кіберзлочину, так й об'єктом, на який він буде спрямований. Саме тому дослідження аспектів прогнозування інформаційних трендів кібератак є актуальною та сучасною темою наукового дослідження.

Формулювання цілей статті. Метою даної статті є побудова моделей класу авторегресії для прогнозування інформаційних трендів кібератак, що дозволить сформувати стратегію їх протидії та зменшити вплив негативних наслідків.

Виклад основного матеріалу дослідження. Для реалізації поставленої мети дослідження було сформовано набір даних за період з 28.01.2018 по 22.01.2023, який включає три види кібератак у вигляді соціальної інженерії, DoS-атак та атак на паролі користувачів. Інформацію було узято із веб-сайту Google Trends, яка відображає кількість запитів користувачів глобальної мережі щодо певного об'єкту чи проблеми. Оскільки виявлення наслідків кібератак конкретним суб'єктом економіки може тривати у часі в залежності від можливостей його системи безпеки та моніторингу, то обрана інформація щодо запитів показує миттєві реакції користувачів у всьому світі щодо кіберзлочинів. Як правило, їх кількість зростає після здійснення кіберзлочину, в іншому випадку, користувачі є менш активними та цікавляться інформацією щодо кіберзагроз в меншій мірі. Тому дані інформаційні тренди є індикаторами потенційних кіберзлочинів для всього світу. Розрахунки проводилися із застосуванням мови програмування Python.

На рисунках 1-3 представлена динаміка трьох видів кіберзагроз. Аналізуючи графіки можна сказати, що обрані дані є часовими рядами. DoS-атаки не мають чітко вираженої тенденції та сезонності (рис. 1) і скоріше за все ряд є стаціонарним. Соціальна інженерія має сезонність та тенденцію (рис. 2) і тому, можливо, ряд є нестаціонарним. Атаки на паролі користувачів показують ймовірну наявність тенденції (рис. 3). Дані висновки потребують подальшого тестування та перевірки.

Спочатку обрані ряди було перевірено на відповідність нормальному розподілу, для чого було проведено тест Харке-Бера. Для DoS-атак p-значення дорівнює 0,0442, що свідчить про відхилення нульової гіпотези про нормальний розподіл. Відповідно, є потреба у здійсненні логарифмування ряду. Але візуальний аналіз гістограми розподілу для даного ряду та перевірка висновку шляхом логарифмування початкових даних дозволили дійти висновку у відсутності доцільності здійснення даної процедури. Для ряду "Соціальна інженерія" було отримано p-значення 0.0247, що також свідчить про відхилення нульової гіпотези про нормальний розподіл. Здійснення процедури логарифмування дозволило підвищити p-значення до 0.4139. Для ряду "Атаки на паролі користувачів" цей показник менше 0,05, що не підтверджує нульову гіпотезу про нормальний розподіл, тому цей факт вимагав здійснення процедури логарифмування початкових даних.

На наступному кроці було проведено перевірку на стаціонарність із використанням розширеного тесту Дики-Фулера. Для усіх рядів критичними значеннями є: 1%: -3.4563; 5%: -2.8729; 10%: -2.5728. Для DoS-атак визначено результати тесту: ADF: -4.0833; P-value: 0.0010. Отримані значення дозволили дійти

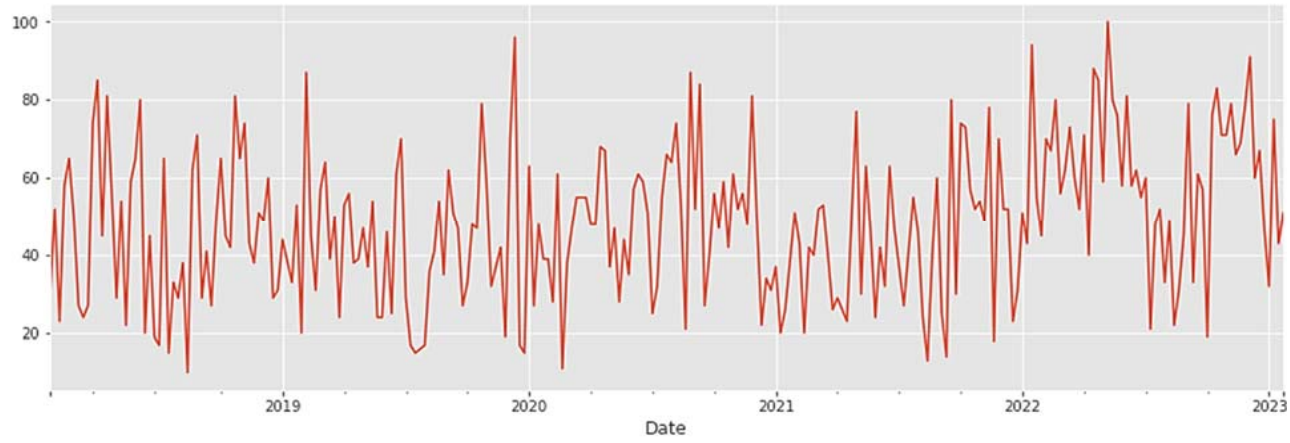

Рис. 1. Графік ряду “DoS-атаки”

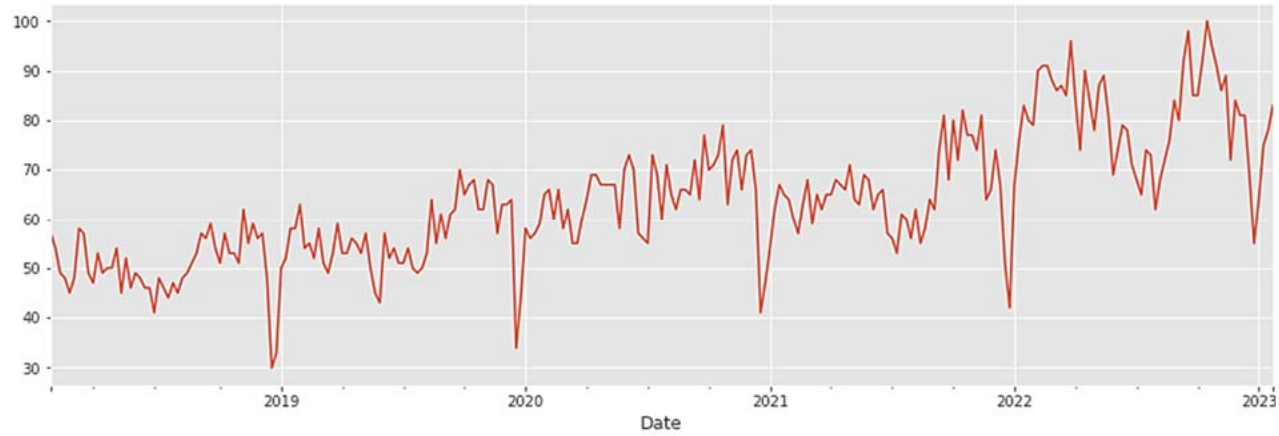

Рис. 2. Графік ряду “Соціальна інженерія”

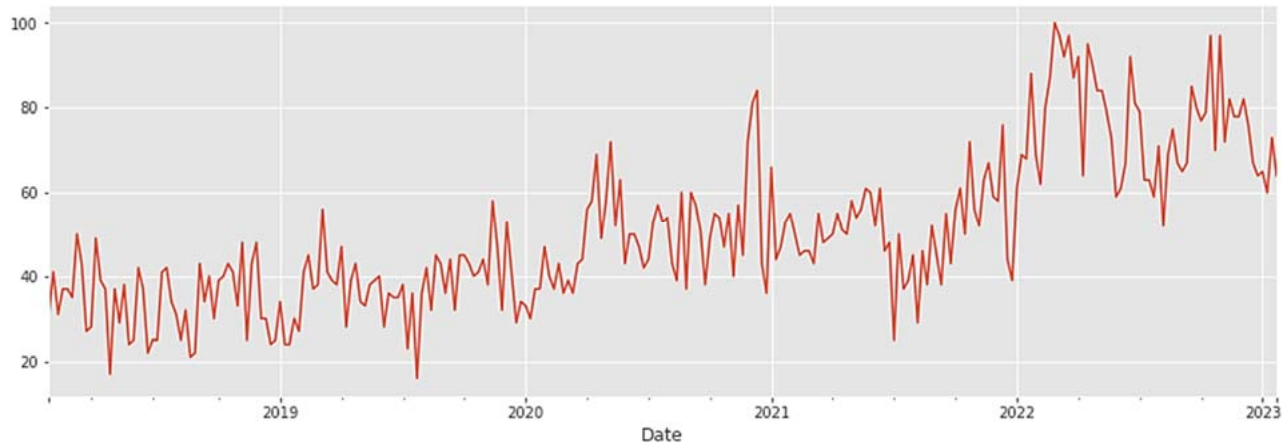

Рис. 3. Графік ряду “Атаки на паролі користувачів”

висновку, що даний досліджуваний ряд є стаціонарним та не має одиничних коренів, тому для побудови авторегресійної моделі потреба у його інтегруванні відпадає. Для ряду “Соціальна інженерія” значення тесту Дики-Фулера є наступними: ADF: -2.8748; P-value: 0.0484. Результати показали, що ряд є також стаціонарним та не має одиничних коренів, тому немає потреби у його інтегруванні. Для ряду “Атаки на паролі користувачів” результати є наступними: ADF: -1.9839; P-value: 0.2937. Це свідчить про те, що він є нестаціонарним та має одиничні корені. Тому для даного випадку є необхідність у здійсненні процедури

інтегрування, що сприятиме перетворенню ряду у стаціонарний. Дані висновки було підтверджено повторним проведенням тестування, але вже після процедури інтегрування. В результаті було отримано: ADF: -13.0032; P-value: 0.0000. Тобто, перетворення сприяло створенню стаціонарного ряду.

На наступному кроці було проаналізовано графіки декомпозицій рядів та автокореляційних функцій для трьох видів кібератак з метою виявлення наявності чи відсутності сезонного компоненту, а також виду автокореляційної функції. В результаті проведеного аналізу було встановлено, що ряд “DoS-атаки” не містить сезонності, але містить авторегресійну та складову ковзного середнього, тобто в результаті буде побудовано ARMA-модель. Автокореляційні функції ряду “Соціальна інженерія” дозволили виявити сезонний компонент із лагом 52, а також авторегресійний процес, тому пропонується модель SARIMA. Аналіз для ряду “Атаки на паролі користувачів” також підтвердив наявність сезонності та авторегресійного процесу, що потребує побудову SARIMA-моделі.

З урахуванням отриманих результатів для всіх проведених тестів було побудовано серію моделей для кожного виду інформаційних трендів кібератак та обрано ту, яка є найкращою за інформаційними показниками AIC, BIC та HQIC. Результати представлені на рисунках 4-6.

Проаналізуємо отримані результати для ряду “DoS-атаки”. На рисунку 4 можна побачити, що було отримано ARMA-модель, яка містить авторегресію 3-го порядку та ковзне середнє 3-го порядку. Кожна складова моделі є статистично значущою, оскільки визначені для них p-значення менші 0,05. Ймовірність для Люнга-Бокса вище 0,05, тому ми не можемо відхилити гіпотезу, що помилки є білим шумом. Значення p-статистики для гетероскедастичності також вище 0,05, що свідчить про гомоскедастичність залишків. Виходячи із того, що результати даної моделі було обрано за найкращими значеннями інформаційних критеріїв, то можна сказати, що її оцінки є статистично значущими, а залишки некорельовані та із постійною дисперсією. Дана модель є ефективною для прогнозування.

Проведемо аналіз результатів для ряду “Соціальна інженерія”. Рисунок 5 показує, що було отримано модель, яка містить авторегресію 1-го порядку, сезонну компоненту із лагом 52, для якої існує ковзна середня 1-го порядку. Статистичну значущість кожної складової моделі підтверджує p-значення, яке є меншим ніж 0,05. Ймовірність для Люнга-Бокса нижче 0,05, тому ми відхиляємо гіпотезу, що помилки є білим шумом. Але розрахунок даного параметру для кожного спостереження дозволив виявити, що на це впливає наявність сезонної складової.

SARIMAX Results

Dep. Variable:	DoS	No. Observations:	261
Model:	SARIMAX(3, 0, 3)	Log Likelihood	-1137.549
Date:	Wed, 01 Feb 2023	AIC	2289.098
Time:	18:34:18	BIC	2314.049
Sample:	01-28-2018 - 01-22-2023	HQIC	2299.127
Covariance Type:	opg		

	coef	std err	z	P>|z|	[0.025	0.975]
ar.L1	-0.4065	0.037	-10.995	0.000	-0.479	-0.334
ar.L2	0.4490	0.030	14.811	0.000	0.390	0.508
ar.L3	0.9571	0.041	23.078	0.000	0.876	1.038
ma.L1	0.5176	0.044	11.850	0.000	0.432	0.603
ma.L2	-0.3562	0.043	-8.200	0.000	-0.441	-0.271
ma.L3	-0.9166	0.054	-17.036	0.000	-1.022	-0.811
sigma2	347.2051	36.900	9.409	0.000	274.883	419.528

Ljung-Box (L1) (Q):	0.85	Jarque-Bera (JB):	3.77
Prob(Q):	0.36	Prob(JB):	0.15
Heteroskedasticity (H):	1.12	Skew:	0.17
Prob(H) (two-sided):	0.61	Kurtosis:	2.52

Рис. 4. Побудова ARMA моделі для ряду “DoS-атаки”

SARIMAX Results

Dep. Variable:	SE	No. Observations:	261
Model:	SARIMAX(1, 0, 0)x(1, 0, [1], 52)	Log Likelihood	196.982
Date:	Wed, 01 Feb 2023	AIC	-385.965
Time:	18:59:51	BIC	-371.707
Sample:	01-28-2018 - 01-22-2023	HQIC	-380.233
Covariance Type:	opg		

	coef	std err	z	P>|z|	[0.025	0.975]
ar.L1	0.9999	0.000	6768.409	0.000	1.000	1.000
ar.S.L52	0.7462	0.110	6.776	0.000	0.530	0.962
ma.S.L52	-0.4378	0.152	-2.880	0.004	-0.736	-0.140
sigma2	0.0119	0.001	12.168	0.000	0.010	0.014

Ljung-Box (L1) (Q):	26.01	Jarque-Bera (JB):	38.07
Prob(Q):	0.00	Prob(JB):	0.00
Heteroskedasticity (H):	0.99	Skew:	-0.25
Prob(H) (two-sided):	0.98	Kurtosis:	4.80

Рис. 5. Побудова SARIMA моделі для ряду “Соціальна інженерія”

SARIMAX Results

Dep. Variable:	PA	No. Observations:	261
Model:	SARIMAX(4, 1, 0)x(1, 1, 0, 52)	Log Likelihood	-20.531
Date:	Wed, 01 Feb 2023	AIC	53.061
Time:	18:13:15	BIC	73.087
Sample:	01-28-2018 - 01-22-2023	HQIC	61.159
Covariance Type:	opg		

	coef	std err	z	P>|z|	[0.025	0.975]
ar.L1	-0.7478	0.068	-10.989	0.000	-0.881	-0.614
ar.L2	-0.4684	0.070	-6.675	0.000	-0.606	-0.331
ar.L3	-0.3102	0.071	-4.372	0.000	-0.449	-0.171
ar.L4	-0.2429	0.061	-3.976	0.000	-0.363	-0.123
ar.S.L52	-0.5677	0.055	-10.240	0.000	-0.676	-0.459
sigma2	0.0645	0.007	9.449	0.000	0.051	0.078

Ljung-Box (L1) (Q):	0.02	Jarque-Bera (JB):	0.21
Prob(Q):	0.88	Prob(JB):	0.90
Heteroskedasticity (H):	0.50	Skew:	0.05
Prob(H) (two-sided):	0.00	Kurtosis:	3.11

Рис. 6. Побудова SARIMA моделі д
ля ряду “Атаки на паролі користувачів”

Для всіх інших спостережень автокореляція відсутня. Р-статистика для гетероскедастичності вище 0,05, що свідчить про гомоскедастичність залишків. Склад моделі було обрано за найкращими значеннями інформаційних критеріїв, то можна зробити висновок, що модель має статистично значущі оцінки її параметрів, гомоскедастичні залишки, але присутня автокореляція між ними, що може впливати на певну зміщеність оцінок. Оскільки застосування різних комбінацій не дозволило покращити параметри моделі, то верифікація результатів прогнозування дозволить прийняти остаточне рішення щодо її якості.

Проаналізуємо результати для ряду “Атаки на паролі користувачів”. На рисунку 6 можна побачити, що було отримано модель, яка містить авторегресію 4-го порядку, сезонну складову із лагом 52. При цьому враховується також й порядок інтеграції 1. Всі складові моделі є статистично значущими (р-значення менші 0,05). Ймовірність для Люнга-Бокса вище 0,05, тому гіпотеза, що помилки є білим шумом, не відхиляється. Р-статистика для гетероскедастичності є менше ніж 0,05, тому ми відхиляємо гіпотезу про гомоскедастичність залишків. Результати даної моделі обиралися за найкращими значеннями інформаційних критеріїв, то вона має статистично значущі оцінки, неко-

рельовані, але гетероскедастичні залишки. Її ефективність для прогнозування буде підтверджено або відхилено шляхом визначення показників оцінки якості прогнозів.

Для прогнозування набори даних було поділено на тестову та верифікаційну вибірки. Безпосередньо його результати представлено на рисунках 7-9.

У таблиці 1 наведено розраховані показники якості прогнозів, які свідчать про можливості застосування побудованих моделей на практиці. Рисунок 7 показує, що прогнозна модель ряду “DoS-атаки” за своєю формою нагадує ковзну середню, але це є очікувано, оскільки вона містить її компонент. Верифікація прогнозних результатів свідчить, що рівень моделі

Рис. 7. Прогноз для ряду “DoS-атаки”

Рис. 8. Прогноз для ряду “Соціальна інженерія”

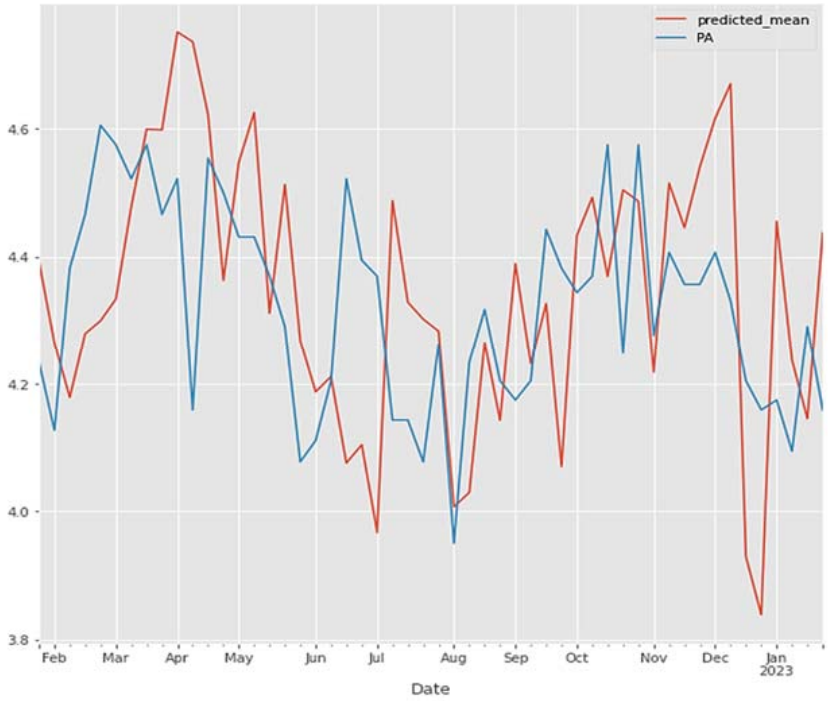

Рис. 9. Прогноз для ряду “Атаки на паролі користувачів”

є між добрим та задовільним, на що вказують значення показників оцінки якості прогнозів (табл. 1). Оскільки обрана прогнозна модель підтвердила всі тести, то її можна використовувати для прогнозування DoS-атак.

Візуалізація результатів прогнозування ряду “Соціальна інженерія” на рисунку 8, показує досить гарні результати співпадіння модельованих та фактичних значень, які також враховують й сезонну компоненту. Значення оцінок якості прогнозів (твбл. 1) знаходяться на високому рівні та підтверджують, що прогноз є високої якості. Хоча побудована модель не пройшла тест на автокорельованість залишків, але при цьому вона видає гарні результати прогнозів, то приходимо до висновку щодо доцільності її застосування для прогнозування кіберзлочинів, пов’язаних із соціальною інженерією.

Результати прогнозування ряду “Атаки на паролі користувачів” представлені на рисунку 9, де чітко можна побачити, що у більшості випадків модель видає правильні результати. Розрахунок показників якості прогнозів (табл. 1) показує, що прогноз можна віднести до високоякісних, оскільки всі показники наближаються до нульових значень, а MAPE є меншим ніж 5%. Оскільки модель не пройшла перевірку на гетероскедастичність, то її оцінки мають завищені значення, що також може вплинути на результативність. Тому модель потребує доопрацювання в майбутньому.

Висновки. Проблема кіберзлочинності є актуальною у наш час, оскільки її масовість та масштабність може впливати на розвиток економіки в країні шляхом формування вразливостей за рахунок її тінізації, відмивання доходів, отриманих злочинним шляхом, підтримки Даркнету, тощо. Дане питання потребує систематичного дослідження та розробки відповідних превентивних заходів, оскільки

Таблиця 1

Результати верифікації прогнозів

Показники верифікації	DoS-атаки	Соціальна інженерія	Атаки на паролі користувачів
RMSE	19,2421	0,0887	0,2163
MAE	16,1291	0,0720	0,1818
MSE	370,2588	0,0079	0,0468
MAPE	28,0861%	1,6595%	4,2026%

характер злочинів, об'єкти та інструментарій їх здійснення постійно змінюються. Тому розробка прогнозних моделей інформаційних трендів кібератак є актуальною темою.

Дана стаття базувалася на дослідженні емпіричних даних, отриманих на основі даних Google Trends, оскільки ця інформація є свідченням реакцій користувачів глобальної мережі на масовість кіберзлочинів. Було обрано три види найпоширених видів кібератак, пов'язаних із соціальною інженерією, DoS-атаками та атаками на паролі користувачів. Процес прогнозування передбачив здійснення тестів Харке-Бера, Дики-Фулера, аналіз гістограм розподілу, декомпозиції часового ряду та автокореляційних функцій для підтвердження чи відхилення гіпотез про нормальність, стаціонарність, наявність сезонної компоненти та вибір структури моделі. В результаті було побудовано для ряду DoS-атакам ARMA-модель, яка містить процеси авторегресії та ковзного середнього 3-го порядку. Тестування залишків та якості прогнозів даної моделі дозволили встановити, що її якість є задовільною при статистичній значущості параметрів, відсутності автокореляції та гетероскедастичності залишків. В цілому, її використання дозволить зробити прогноз середньої якості.

Для ряду "Соціальна інженерія" побудовано SARIMA-модель, яка містить авторегресійний процес 1-го порядку, сезонну компоненту та ковзну середню 1-го порядку для неї. Візуалізація прогнозів та оцінка їх якості показала, що модель демонструє гарні результати. Але тест Люнга-Бокса підтвердив наявність автокореляції залишків. Оскільки розраховане значення для прогнозних спостережень не виявила її, то на даний результат вплинула наявність сезонної компонент із значним лагом, що потребує збільшення вибірки дослідження. Не дивлячись на даний нюанс, модель можна використовувати для прогнозування кіберзлочинів, пов'язаних із соціальною інженерією. Для ряду "Атаки на паролі користувачів" було побудовано SARIMA-модель із авторегресійним процесом та сезонною складовою. При цьому ряд було проінтегровано, оскільки його значення є нестаціонарними. Хоча верифікація прогнозів показала високу якість моделі, але її залишки є гетероскедастичними, що вплинуло на завищення оцінок її параметрів. Тому модель потребує проведення модифікації.

Отримані результати даного дослідження можна використовувати для удосконалення стратегічних планів країни щодо формування комплексу превентивних заходів для попередження кіберзагроз. Також це потребуватиме створення динамічної бази статистичних даних на основі відкритих та закритих джерел офіційних даних, які стосуються різних видів масових кіберзлочинів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Kokaji A., Goto A. An analysis of economic losses from cyberattacks: based on input–output model and production function. *Journal of Economic Structures.* 2022. Vol. 11. № 1. Art. num. 34. DOI: https://doi.org/10.1186/s40008-022-00286-4.

2. Tian S., Zhao B., Olivares R.O. Cybersecurity risks and central banks' sentiment on central bank digital currency: Evidence from global cyberattacks. *Finance Research Letters*. 2023. Vol. 53. Art. num. 103609. DOI: https://doi.org/10.1016/j.frl.2022.103609.

3. Klumpes P. Coordination of cybersecurity risk management in the U.K. insurance sector. *Geneva Papers on Risk and Insurance: Issues and Practice.* 2023. Vol. 48, № 2. P. 332–371. DOI: https://doi.org/10.1057/s41288-023-00287-9.

4. Heymann F., Henry S., Galus M. Cybersecurity and resilience in the swiss electricity sector: Status and policy options. *Utilities Policy.* 2022. Vol. 79. Art. num. 101432. DOI: https://doi.org/10.1016/j.jup.2022.101432.

5. Gafni R., Pavel T. Cyberattacks against the health-care sectors during the COVID-19 pandemic. *Information and Computer Security.* 2022. Vol. 30, № 1. P. 137–150. DOI: https://doi.org/10.1108/ICS-05-2021-0059.

6. Kirimhan D. Importance of anti-money laundering regulations among prosumers for a cybersecure decentralized finance. *Journal of Business Research.* 2023. Vol. 157. Art. num. 113558. DOI: https://doi.org/10.1016/j.jbusres.2022.113558.

7. Paraskevas A. Cybersecurity in travel and tourism: a risk-based approach. In *Handbook of e-Tourism.* Cham: Springer International Publishing, 2022. P. 1605–1628.

8. Punt E., Monstadt J., Frank S., Witte P. Navigating cyber resilience in seaports: challenges of preparing for cyberattacks at the Port of Rotterdam. *Digital Policy, Regulation and Governance.* 2023. In press. DOI: https://doi.org/10.1108/DPRG-12-2022-0150

9. Baliker C., Baza M., Alourani A., Alshehri A., Alshahrani H., Choo K.R. On the Applications of Blockchain in FinTech: Advancements and Opportunities. *IEEE Transactions on Engineering Management.* 2023. P. 1–18. In press. DOI: https://doi.org/10.1109/TEM.2022.3231057.

10. Fan S., Yang Z. Safety and security co-analysis in transport systems: Current state and regulatory development. *Transportation Research Part A: Policy and Practice.* 2022. Vol. 166. P. 369–388. DOI: https://doi.org/10.1016/j.tra.2022.11.005.

11.Sánchez M. A., De Batista M. Business continuity for times of vulnerability: Empirical evidence. *Journal of Contingencies and Crisis Management.* 2023. In press. DOI: https://doi.org/10.1111/1468-5973.12449.

12. Crosignani M., Macchiavelli M., Silva A.F. Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics.* 2023. Vol. 147, № 2. P. 432–448. DOI: https://doi.org/10.1016/j.jfineco.2022.12.002.

REFERENCES:

1. Kokaji, A., & Goto, A. (2022). An analysis of economic losses from cyberattacks: based on input–output model and production function. *Journal of Economic Structures, 11*(1), 34. DOI: https://doi.org/10.1186/s40008-022-00286-4.

2. Tian, S., Zhao, B., & Olivares, R.O. (2023). Cybersecurity risks and central banks' sentiment on central bank digital currency: Evidence from global cyberattacks. *Finance Research Letters*, *53*,103609. DOI: https://doi.org/10.1016/j.frl.2022.103609.

3. Klumpes, P. (2023). Coordination of cybersecurity risk management in the U.K. insurance sector. *Geneva Papers on Risk and Insurance: Issues and Practice, 48*(2), 332–371. DOI: https://doi.org/10.1057/s41288-023-00287-9.

4. Heymann, F., Henry, S., & Galus, M. (2022). Cybersecurity and resilience in the swiss electricity sector: Status and policy options. *Utilities Policy, 79*, 101432. DOI: https://doi.org/10.1016/j.jup.2022.101432.

5. Gafni, R., & Pavel, T. (2022). Cyberattacks against the health-care sectors during the COVID-19 pandemic. *Information and Computer Security, 30*(1), 137–150. DOI: https://doi.org/10.1108/ICS-05-2021-0059.

6. Kirimhan, D. (2023). Importance of anti-money laundering regulations among prosumers for a cybersecure decentralized finance. *Journal of Business Research, 157*, 113558. DOI: https://doi.org/10.1016/j.jbusres.2022.113558.

7. Paraskevas, A. (2022). Cybersecurity in travel and tourism: a risk-based approach. In *Handbook of e-Tourism* (pp. 1605–1628). Cham: Springer International Publishing.

8. Punt, E., Monstadt, J., Frank, S., & Witte, P. (2023). Navigating cyber resilience in seaports: challenges of preparing for cyberattacks at the Port of Rotterdam. *Digital Policy, Regulation and Governance,* in press. DOI: https://doi.org/10.1108/DPRG-12-2022-0150

9. Baliker, C., Baza, M., Alourani, A., Alshehri, A., Alshahrani, H., & Choo, K.R. (2023). On the Applications of Blockchain in FinTech: Advancements and Opportunities. *IEEE Transactions on Engineering Management,* 1-18, in press. DOI: https://doi.org/10.1109/TEM.2022.3231057.

10. Fan, S., & Yang, Z. (2022). Safety and security co-analysis in transport systems: Current state and regulatory development. *Transportation Research Part A: Policy and Practice, 166*, 369–388. DOI: https://doi.org/10.1016/j.tra.2022.11.005.

11.Sánchez, M. A., & De Batista, M. (2023). Business continuity for times of vulnerability: Empirical evidence. *Journal of Contingencies and Crisis Management,* in press. DOI: https://doi.org/10.1111/1468-5973.12449.

12. Crosignani, M., Macchiavelli, M., & Silva, A.F. (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics, 147*(2), 432–448. DOI: https://doi.org/10.1016/j.jfineco.2022.12.002.