

Список використаних джерел

1. Про введення воєнного стану в Україні: Указ Президента України від 24 лют. 2022 р. № 64/2022. URL: <https://zakon.rada.gov.ua/laws/show/64/2022>.
2. Кримінальний процесуальний кодекс України від 13 квіт. 2012 р. № 4651-VI. URL: <https://zakon.rada.gov.ua/laws/show/4651-17>.
3. Про електронні документи та електронний документообіг: Закон України від 22 трав. 2003 р. № 851-IV. URL: <https://zakon.rada.gov.ua/laws/show/851-15>.
4. Романюк В. В., Абламський С. Є. Критерії допустимості цифрових (електронних) доказів у кримінальному провадженні. *Право і безпека*. 2024. № 2 (93). С. 96–104.
5. Верховний Суд. Суддя ВС проаналізувала критерії допустимості й достовірності електронних доказів у кримінальному процесі. 06.02.2025. URL: <https://supreme.court.gov.ua/supreme/pres-centr/news/1751385>.
6. UN Office of the High Commissioner for Human Rights; University of California, Berkeley, Human Rights Center. Berkeley Protocol on Digital Open Source Investigations. New York; Geneva: OHCHR, 2022. URL: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>.
7. Електронні докази як об'єкт експертного дослідження в кримінальних провадженнях щодо воєнних злочинів. *Криміналістика та судова експертиза у XXI столітті* : матеріали Всеукраїнського науково-практичного семінару (м. Київ, 30 травня 2024 року). Київ : ДНДЕКЦ МВС України, 2024. С. 279–282.
8. Вплив цифровізації судочинства на якість доказування у кримінальному провадженні. *Academy Vision*. 2024. URL: <https://academy-vision.org/index.php/av/article/download/2729/2575>.
9. Кримінальне судочинство в умовах дії правового режиму воєнного стану: електронні докази. Наукові матеріали НАВС України. URL: <https://elar.navs.edu.ua>.

Степанов Анатолій Анатолійович, курсант ХНУВС

Науковий керівник – **Тімошин Анатолій Сергійович**, доцент кафедри інформаційних систем та технологій навчально-наукового інституту № 4 ХНУВС, кандидат фізико-математичних наук, доцент

АВТОМАТИЗОВАНИЙ ВІДБІР ПІДОЗРІЛИХ ВЕБРЕСУРСІВ У МАСИВАХ URL-ДАНИХ

Розвиток інформаційних технологій та глобалізація інтернет-простору зумовили стрімке зростання кількості вебресурсів, серед яких значну частку становлять шкідливі та підозрілі сайти. Автоматизований відбір таких ресурсів у масивах URL-даних є актуальним науково-практичним завданням у сфері кібербезпеки.

Метою дослідження є розроблення підходів до автоматизованого аналізу та класифікації URL-адрес для виявлення потенційно небезпечних вебресурсів без необхідності звернення до самих сайтів, що дозволяє суттєво знизити ризики для кінцевих користувачів та інформаційних систем.

Аналіз наукових джерел свідчить про те, що для вирішення зазначеної задачі застосовуються методи машинного навчання, зокрема алгоритми бінарної класифікації – логістична регресія, метод опорних векторів (SVM), випадковий ліс (Random Forest), а також нейронні мережі [1, с. 112]. Вхідними даними для таких моделей слугують ознаки, отримані безпосередньо з тексту URL-адреси, без активації ресурсу.

У рамках дослідження визначено такі ключові ознаки URL-адреси, що корелюють із підозрілістю ресурсу: довжина URL та окремих її складових (домен, шлях, запит); кількість спеціальних символів («@», «-», «_», «%»); наявність IP-адреси замість доменного імені; використання підозрілих ключових слів («login», «secure», «verify», «account»); кількість піддоменів; застосування URL-шортерів; ентропія рядка як індикатор випадково згенерованих символів [2, с. 47]. Для формування навчальної вибірки використано публічні набори даних, зокрема PhishTank та DMOZ, що містять мітки «фішингові» та «легітимні» URL-адреси. Після попередньої обробки та балансування класів сформовано вибірку обсягом понад 50 000 записів. Отримані результати свідчать, що найвищу точність класифікації – 97,3 % – демонструє алгоритм Random Forest при використанні всіх виділених ознак.

Практична значущість роботи полягає у можливості інтеграції розробленого модуля у системи моніторингу мережевого трафіку та браузерні розширення для превентивного блокування підозрілих ресурсів у режимі реального часу. Це сприятиме підвищенню рівня кіберзахисту як окремих користувачів, так і корпоративних інформаційних систем.

Отже, автоматизований URL-аналіз на основі методів машинного навчання є ефективним інструментом виявлення підозрілих вебресурсів. Перспективним напрямом подальших досліджень є розширення ознакового простору за рахунок аналізу WHOIS-даних та сертифікатів SSL, а також тестування моделей на більш різноманітних та актуальних наборах даних.

Розвиток інформаційних технологій та глобалізація інтернет-простору зумовили стрімке зростання кількості вебресурсів, серед яких значну частку становлять шкідливі та підозрілі сайти. Автоматизований відбір таких ресурсів у масивах URL-даних є актуальним науково-практичним завданням у сфері кібербезпеки. Особливої актуальності ця проблема набуває в умовах постійного зростання кількості фішингових атак, спрямованих на викрадення конфіденційної інформації користувачів, зокрема облікових даних, банківських реквізитів та персональних даних.

Додатково варто враховувати такі фактори, як вік домену, наявність SSL-сертифіката, а також частота появи URL у чорних списках, що може значно підвищити точність моделей. Крім того, перспективним є застосування методів глибокого навчання для автоматичного вилучення ознак.

Список використаних джерел

1. Sahoo D., Liu C., Hoi S. C. H. Malicious URL Detection using Machine Learning: A Survey. arXiv preprint arXiv:1701.07179. 2017. 18 p.
2. Mamun M. S. I., Rathore M. A., Lashkari A. H. et al. Detecting Malicious URLs Using Lexical Analysis. *Network and System Security*. 2016. P. 38–55.
3. Le A., Markopoulou A., Faloutsos M. PhishDef: URL Names Say It All. *IEEE INFOCOM*. 2011. P. 191–195.
4. Blum A., Wardman B., Solorio T., Warner G. Lexical Feature Based Phishing URL Detection Using Online Learning. *Proceedings of the 3rd ACM Workshop on Artificial Intelligence and Security*. 2010. P. 54–60.

Ступак Аркадій Володимирович, курсант НАВС

Науковий керівник – **Гусєва Катерина Анатоліївна**, доцент кафедри поліцейської діяльності НАВС, кандидат юридичних наук, старший науковий співробітник

АДМІНІСТРАТИВНА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ВІЙСЬКОВИЙ ОБОВ'ЯЗОК І МОБІЛІЗАЦІЮ: ПРОБЛЕМИ ПРАВОЗАСТОСУВАННЯ

На сьогоднішній день питання мобілізації та відповідальності за порушення її правил є одним з основних та першочергових питань, які постали перед українським суспільством, оскільки за весь час воєнного стану інтенсивність застосування норм, що передбачають адміністративну відповідальність за порушення законодавства про військовий обов'язок та мобілізацію постійно зростає. Так лише за 2025 рік було відкрито понад 28 тисяч проваджень за порушення правил мобілізації [3].

Сьогодні в Україні за порушення правил мобілізації передбачається кримінальна відповідальність та адміністративна відповідальність за ст. 210, 210-1 КУпАП[1]. Адміністративна відповідальність є первинним механізмом реагування держави на порушення законодавства про військовий обов'язок та мобілізацію, через що в межах даного дослідження доцільним буде розглянути саме адміністративну відповідальність.

Це питання неодноразово привертало увагу ряду науковців, які намагалися дати на нього відповідь. Зокрема, В. М. Братковський у своїх дослідженнях зазначав, що розвиток інституту адміністративної відповідальності у сфері мобілізації безпосередньо залежав від змін безпекової ситуації та посилення ролі держави у сфері оборони [4, с. 215–217]. Однак його дослідження стосуються скоріш історичного розвитку, а більш практичний підхід простежується у працях О. С. Володавської, яка дослідила процес розмежування