

enshrined in Article 8 of the Constitution of Ukraine [1], must remain the foundational constraint on all national security measures, including those adopted under martial law conditions.

Thus, ensuring national security in the contemporary context demands a comprehensive approach that unites constitutional guarantees, effective law enforcement mechanisms, and deep integration into international security frameworks. The Ukrainian experience under martial law offers both lessons and challenges that are of broader relevance for the development of national security doctrine. Further research should focus on the empirical assessment of institutional reforms undertaken since 2022 and on the development of evidence-based recommendations for the post-war reconstruction of Ukraine's security sector, with particular attention to the harmonization of domestic legislation with EU and NATO standards and the institutionalization of preventive security approaches.

References

1. Constitution of Ukraine of June 28, 1996. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр>
2. Law of Ukraine «On National Security of Ukraine» of June 21, 2018 No. 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19>
3. Law of Ukraine «On Combating Terrorism» of March 20, 2003 No. 638-IV. URL: <https://zakon.rada.gov.ua/laws/show/638-15>
4. Criminal Code of Ukraine of April 5, 2001 No. 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14>
5. National Security Strategy of Ukraine, approved by Decree of the President of Ukraine No. 392/2020 of September 14, 2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020>
6. HM Government. Counter-Terrorism Strategy (CONTEST) 2023. London : Home Office, 2023. 116 p.
7. Horbulin V. P. National Security of Ukraine: Challenges and Priorities. Kyiv : NISD, 2021. 224 p.
8. Thornton R. Asymmetric Warfare: Threat and Response in the 21st Century. Cambridge : Polity Press, 2021. 256 p.
9. Kolesnik S. P. Legal Provision of Prevention of Terrorism by National Police. *European Reforms Bulletin*. 2019. No. 3. P. 28–32.
10. U.S. Department of State. Country Reports on Terrorism 2023. Washington : Bureau of Counterterrorism, 2024. 312 p.
11. Online Safety Act 2023, c. 50 (UK). URL: <https://www.legislation.gov.uk/ukpga/2023/50>.

Ганусяк Богдан Володимирович, курсант ХНУВС

Науковий керівник – **Тімошин Анатолій Сергійович**, доцент кафедри інформаційних систем та технологій ХНУВС, кандидат фізико-математичних наук, доцент

ВИЯВЛЕННЯ ПІДОЗРІЛИХ ШАБЛОНІВ У ДОМЕННИХ ІМЕНАХ ВЕБРЕСУРСІВ

У сучасних умовах стрімкого розвитку інформаційних технологій питання забезпечення кібербезпеки набуває особливої актуальності [1, с. 205]. Значна частина сучасних кіберзагроз пов'язана із використанням шкідливих вебресурсів, які створюються з метою викрадення конфіденційної інформації та отримання несанкціонованого доступу до облікових записів користувачів. Одним із важливих елементів будь-якого вебресурсу є доменне ім'я, яке виконує роль унікального ідентифікатора ресурсу в мережі Інтернет. Саме тому аналіз доменних імен є ефективним інструментом для виявлення потенційно небезпечних вебресурсів і протидії кіберзлочинності.

Сьогодні зловмисники активно використовують різноманітні методи маскуванню шкідливих сайтів під легітимні вебресурси. Найчастіше такі домени створюються таким чином, щоб бути максимально схожими на адреси популярних сервісів, банківських установ або соціальних мереж. Основною метою подібних дій є введення користувача в оману та спонукання його перейти на фальшивий ресурс. Після переходу користувач може несвідомо ввести персональні дані, логіни чи банківські реквізити, які надалі використовуються зловмисниками [2, с. 53]. Такі атаки є одними з найпоширеніших способів реалізації фішингових схем у мережі Інтернет.

Одним із найбільш поширених способів створення підозрілих доменів є тайпсквотинг. Цей метод полягає у реєстрації доменних імен, які містять навмисні помилки у написанні відомих вебадрес. Наприклад, замість адреси «google.com» може використовуватись

«google.com» або «gogle.com». Користувачі часто не помічають подібних змін через неувважність, що робить такі атаки достатньо ефективними [3]. Подібні схеми використовуються і щодо банківських сервісів, електронної пошти та інших популярних платформ.

Ще одним способом маскування доменів є використання гомографічних атак. Суть даного методу полягає у застосуванні символів різних алфавітів, які зовні виглядають однаково. Наприклад, кирилична літера «а» практично не відрізняється від латинської «a». Крім цього, зловмисники часто використовують довгі доменні імена із великою кількістю додаткових слів або піддоменів. Наприклад, у домені можуть використовуватись слова: «secure», «login», «verify» або «account», які викликають довіру у користувачів. Такі доменні імена створюють хибне враження безпечного або офіційного вебресурсу.

Для виявлення підозрілих шаблонів у доменних іменах використовуються різні методи аналізу. Одним із базових методів є лексичний аналіз, який передбачає дослідження структури доменного імені, кількості символів та використання спеціальних знаків. Наприклад, надмірна довжина домену або велика кількість дефісів може бути ознакою шкідливого ресурсу. Також аналізується частота використання окремих слів та символів у доменних іменах. Важливим етапом є порівняння нових доменів із базою вже відомих небезпечних вебресурсів.

Поширеним методом є перевірка схожості доменного імені із відомими легітимними ресурсами. Для цього використовуються спеціальні алгоритми порівняння рядків, серед яких особливе місце займає алгоритм відстані Левенштейна [2, с. 94]. Даний алгоритм дозволяє автоматично виявляти потенційні фішингові домени, які імітують популярні вебресурси. Чим меншою є різниця між доменними іменами, тим більшою є ймовірність використання домену у шахрайських цілях.

Окрему роль у процесі виявлення небезпечних вебресурсів відіграє аналіз WHOIS-інформації. За допомогою WHOIS можна отримати дані про дату реєстрації домену, країну реєстрації та реєстратора. Практика показує, що значна кількість шкідливих доменів реєструється на короткий термін та використовується лише протягом обмеженого часу [1, с. 213]. Крім того, зловмисники часто приховують інформацію про власника домену або використовують анонімні сервіси реєстрації.

Сучасні системи кібербезпеки також активно використовують технології машинного навчання для автоматичного виявлення підозрілих доменів. На основі аналізу великої кількості характеристик система навчається визначати ознаки, характерні для фішингових або шкідливих ресурсів [3]. Використання подібних технологій дозволяє значно підвищити ефективність автоматизованого виявлення кіберзагроз. Подібні системи можуть функціонувати у режимі реального часу та автоматично блокувати підозрілі вебресурси.

Важливу роль у протидії використанню підозрілих доменів відіграють правоохоронні органи та спеціалізовані підрозділи кіберполіції. Виявлення та блокування фішингових ресурсів дозволяє зменшити кількість кіберзлочинів та запобігти витоку конфіденційної інформації. Аналіз доменних імен також може використовуватись для документування протиправної діяльності та встановлення зв'язків між окремими вебресурсами.

Отже, виявлення підозрілих шаблонів у доменних іменах вебресурсів є важливим напрямом забезпечення кібербезпеки в сучасному цифровому середовищі. Застосування методів лексичного аналізу, алгоритмів порівняння рядків, WHOIS-аналізу та систем машинного навчання дозволяє ефективно виявляти потенційно небезпечні ресурси та знижувати ризики кіберзагроз [2, с. 149].

Список використаних джерел

1. Попова Д. В., Яременко С. В. Аналіз сучасних кіберзагроз у цифровому середовищі. *Економічний вісник Донбасу*. 2024. № 3 (77). С. 203–216.
2. Stallings W. *Network Security Essentials : Applications and Standards*. 6th ed. Pearson Education, 2017. 816 p.
3. Spaulding J., Upadhyaya S., Mohaisen A. The Landscape of Domain Name Typosquatting: Techniques and Countermeasures // arXiv. 2016. URL: <https://arxiv.org/abs/1603.02767>