УДК 004.056

Д. О. Гнітецька

Ю. В. Баришев

РОЛЬ М'ЯКИХ НАВИЧОК У ЗАБЕЗПЕЧЕННІ ЕФЕКТИВНОЇ РОБОТИ ПЕНТЕСТЕРА

Вінницький національний технічний університет

Анотація

Стаття присвячена дослідженню м'яких навичок, необхідних для ефективної діяльності фахівців із тестування на проникнення (пентестерів) у сфері кібербезпеки. Розглянуто основні професійні стандарти, а також вимоги вакансій IT-компаній. На основі порівняльного аналізу цих джерел визначено ключові м'які навички, такі як комунікація, аналітичне мислення, етична поведінка, адаптивність, співпраця та управління часом. Продемонстровано їх значення для виконання професійних завдань, взаємодії з командами та клієнтами, а також запропоновано рекомендації щодо інтеграції цих навичок у підготовку фахівців і розробку гнучких моделей компетенцій.

Ключові слова: *пентестер, етичний хакер, кібербезпека, м'які навички, професійні стандарти, вакансії.*

Abstract

The article is dedicated to the study of soft skills essential for the effective performance of penetration testers (pentesters) in the field of cybersecurity. It examines key professional standards and the requirements of IT company job vacancies. Based on a comparative analysis of these sources, critical soft skills such as communication, analytical thinking, ethical behavior, adaptability, collaboration, and time management are identified. Their importance for performing professional tasks, interacting with teams and clients is demonstrated, and recommendations are proposed for integrating these skills into the training of specialists and the development of flexible competency models.

Keywords: *penetration tester, ethical hacker, cybersecurity, soft skills, professional standarts, vacancies.*

Вступ

Збільшення кількості кібератак породжує потребу у фахівцях кібербезпеки, які зможуть ефективно цим атакам протистояти. І першим кроком для цього є виявлення слабких місць в інформаційних системах. Відповідно саме цим завданням займаються пентестери (етичні хакери). Якщо для технічних або жорстких навичок фахівців цього напряму науковою спільнотою визначені певні рамки, як-то стандарти професій [стандарт тестувальника, аналітика вразливостей], то рамки м'яких навичок є дещо розмитими. Окрім технічних знань, м'які навички відіграють важливу роль у забезпеченні ефективності роботи пентестера, адже впливають на провадження атак з елементами соціальної інженерії, а також роботу в команді. Метою цього дослідження є покращення підготовки пентестерів шляхом ідентифікації множини м'яких навичок, які визначають ключові компетенції цієї професії..

Результати досліджень

Для збору даних використано описи вакансій від компаній 10Guards [1], IBM [2], Sigma Software [3] та PIN-UP Global [4], отримані з відкритих джерел, таких як офіційні вебсайти компаній або платформа пошуку роботи DOU[5]. Додатково враховано бачення професії, відображене у професійних стандартах (EC-Council CEH[6], ENISA ESCF[7]). Збір даних проводився шляхом контент-аналізу текстів вакансій, що дозволило ідентифікувати згадані м'які навички.

Компанія 10Guards[1] висуває до кандидатів на посаду пентестера вимоги, що поєднують технічні та особистісні якості. Комунікативні навички є критично важливими для взаємодії з клієнтами, чіткого пояснення результатів тестування та презентації рекомендацій. Розуміння психології хакерів дозволяє прогнозувати їхні дії та моделювати реалістичні сценарії атак. Аналітичні здібності необхідні для систематичного виявлення вразливостей і оцінки ризиків. Креативність, кмітливість і здатність

виходити за рамки стандартних підходів сприяють розробці нестандартних рішень для складних завдань. Цікавість і азарт до унікальних проєктів мотивують до безперервного навчання та професійного розвитку. Здатність етично порушувати правила в межах дозволеного допомагає імітувати дії зловмисників, зберігаючи високі моральні принципи. Усвідомлення відповідальності забезпечує коректність у роботі з конфіденційними даними.

Компанія IBM[2] висуває до кандидатів на посаду пентестера вимоги, що поєднують професійні та особистісні якості. Допитливість і відкритість до нової інформації необхідні для вивчення сучасних технологій і методів кібератак. Відкритість до зворотного зв'язку та здатність надавати його колегам сприяють професійному розвитку та ефективній співпраці.

Командна робота з урахуванням різних точок зору забезпечує ефективну взаємодію в проєктах. Сміливість у прийнятті важливих рішень дозволяє швидко реагувати на виклики, а позитивне ставлення та орієнтація на результат мотивують досягати цілей, підвищуючи безпеку систем.

У вакансії на посаду пентестера від компанії Sigma Software[3] акцентовано увагу на низці ключових вимог до кандидатів, які відображають специфіку роботи у сфері кібербезпеки. Передусім, кандидат повинен мати відмінні аналітичні навички, що передбачають здатність систематично аналізувати складні технічні дані, виявляти вразливості в програмному забезпеченні та прогнозувати потенційні ризики. Навички вирішення проблем необхідні для розробки ефективних стратегій тестування та адаптації до нестандартних ситуацій. Проактивність дозволяє пентестерам самостійно ініціювати дії для підвищення безпеки систем. Здатність тісно співпрацювати з командами розробників вимагає ефективної комунікації та вміння перекладати технічні висновки на зрозумілу мову, що сприяє швидкому усуненню вразливостей.

Вимоги до кандидатів на посаду пентестера в компанії PIN-UP Global[4] охоплюють набір ключових компетенцій, необхідних для ефективного виконання професійних обов'язків. Кандидати повинні володіти відмінними комунікативними навичками, що включають як усну, так і письмову взаємодію, забезпечуючи чітке формулювання результатів тестування та взаємодію з командою. Сильні аналітичні здібності є необхідними для оцінки ризиків і виявлення вразливостей у складних системах. Здатність вирішувати проблеми дозволяє розробляти стратегії тестування та долати технічні виклики. Уміння працювати як у команді, так і самостійно сприяє синергії проєктів і відповідальності за індивідуальні завдання. Орієнтація на дедлайни та багатозадачність забезпечує своєчасне виконання завдань у динамічному середовищі. Культурна адаптивність є важливою для роботи в міжнародних командах.

Згідно з Європейською рамкою компетенцій у сфері кібербезпеки (ENISA ESCF)[6], ключовими м'якими навичками для фахівців з тестування на проникнення є креативне та нестандартне мислення, комунікація, презентація та звітування, етичне мислення та відповідальність, адаптивність і гнучкість, емоційний інтелект, а також управління часом і самоорганізація. Креативне та нестандартне мислення є основою для розробки нових підходів до виявлення вразливостей у відповідь на еволюцію кіберзагроз. Комунікація відіграє центральну роль у процесі взаємодії з клієнтами та іншими зацікавленими сторонами, адже пентестер має не лише виявляти вразливості, але й чітко пояснювати їх природу, потенційні наслідки та шляхи усунення. Етичне мислення та відповідальність є невід'ємними для пентестера, оскільки робота з конфіденційними даними та критичними системами вимагає дотримання високих моральних стандартів. Адаптивність і гнучкість дозволяють пентестеру швидко реагувати на зміни в технологіях, методах атак або вимогах клієнтів. Емоційний інтелект допомагає будувати довірливі відносини з колегами та клієнтами, управляти конфліктними ситуаціями та впоратися зі стресом. Управління часом і самоорганізація є критично важливими для виконання завдань у встановлені терміни.

Згідно з положеннями програми EC-Council Certified Ethical Hacking[6], для ефективної роботи пентестера необхідний набір м'яких навичок, які забезпечують успішне виконання завдань у складних технічних і організаційних умовах. Аналітичне мислення є фундаментальною компетенцією, що дозволяє пентестеру систематично аналізувати складні системи, виявляти потенційні вразливості та оцінювати їхній вплив на безпеку. Критичне мислення дає змогу об'єктивно оцінювати інформацію, перевіряти припущення та уникати упередженості. Вирішення проблем є основою діяльності пентестера, адже тестування на проникнення часто пов'язане з непередбачуваними ситуаціями. Увага до деталей має вирішальне значення, оскільки навіть незначна помилка чи пропущена вразливість може спричинити серйозні наслідки. Комунікація та співпраця є важливими, адже пентестери часто працюють у командах. Адаптивність і готовність до навчання є критично важливими в умовах стрімкого розвитку технологій. Етична поведінка становить основу професійної діяльності пентестера,

адже робота з тестування на проникнення передбачає доступ до конфіденційних даних. Управління часом дозволяє раціонально розподіляти ресурси і виконувати завдання в умовах обмеженого часу.

Джерело	**Необхідні м'які навички**
10Guards[1]	Комунікація, аналітичне мислення, креативність, кмітливість, вихід за рамки, цікавість, азарт, етичність, відповідальність, розуміння психології хакерів
IBM[2]	Допитливість, відкритість до нової інформації, відкритість до зворотного зв'язку, командна робота, сміливість, орієнтація на результат, позитивне ставлення
Sigma Software[3]	Аналітичні навички, вирішення проблем, проактивність, комунікація, співпраця, адаптивність, переклад технічних висновків у доступну форму
PIN-UP Global[4]	Комунікація (усна й письмова), аналітичні здібності, вирішення проблем, командна робота, самостійність, орієнтація на дедлайни, багатозадачність, культурна адаптивність
ENISA ESCF[6]	Креативність, нестандартне мислення, комунікація, презентація, звітування, етичне мислення, відповідальність, адаптивність, гнучкість, емоційний інтелект, управління часом, самоорганізація
EC-Council CEH[7]	Аналітичне мислення, критичне мислення, вирішення проблем, увага до деталей, комунікація, співпраця, адаптивність, готовність до навчання, етична поведінка, управління часом

Таблиця 1 – Узагальнений перелік необхідних м'яких навичок.

У результаті аналізу вимог до кандидатів на посаду пентестера, отриманих із даних компаній 10Guards[1], IBM[2], Sigma Software[3], PIN-UP Global[4], а також Європейської рамки компетенцій у сфері кібербезпеки (ENISA ESCF)[6] і програми EC-Council Certified Ethical Hacking[7], визначено множину ключових м'яких навичок найбільш часто згадуваних у цих джерелах. До них належать комунікація, аналітичні здібності, етична поведінка/відповідальність, адаптивність/гнучкість, співпраця/командна робота, управління часом/самоорганізація. Комунікація згадується 5 разів — вона є найчастіше згаданою навичкою, оскільки критично важлива для пояснення результатів тестування, взаємодії з клієнтами та командою. Аналітичне мислення зустрічається 4 рази, що свідчить про важливість здатності до логічного аналізу даних і виявлення вразливостей. Етична поведінка або відповідальність також фігурує 4 рази — це підкреслює значення моральних стандартів у роботі з конфіденційною інформацією. Адаптивність і гнучкість згадані 4 рази, адже технології швидко змінюються, і пентестери мають встигати за ними. Співпраця або командна робота з'являється 4 рази, що вказує на цінність вміння ефективно працювати в команді. Управління часом і самоорганізація згадуються також 4 рази — ці навички потрібні для дотримання дедлайнів і ефективного розподілу ресурсів. Вирішення проблем фігурує 3 рази, креативність і нестандартне мислення, проактивність згадані по 2 рази. Критичне мислення, увага до деталей, емоційний інтелект, цікавість і допитливість, сміливість у прийнятті рішень, позитивне ставлення, а також здатність перекладати технічні висновки у доступну мову — кожна з цих навичок згадується по 1 разу, але всі вони мають вагу в конкретних контекстах і підкреслюють різні аспекти ефективності пентестера.

На основі аналізу пропонується включити до професійних стандартів пентестерів такі м'які навички, які мають прямий зв'язок із технічними завданнями: комунікація та співпраця забезпечують ефективне звітування та координацію з командами, аналітичне та критичне мислення підтримують аналіз систем і оцінку ризиків, креативність і нестандартне мислення сприяють пошуку неочевидних вразливостей, вирішення проблем допомагають долати технічні перешкоди, етична поведінка та відповідальність гарантують дотримання етичних і правових норм, адаптивність і здатність до навчання необхідні для освоєння нових технологій, управління часом і самоорганізація забезпечують виконання завдань у межах дедлайнів, увага до деталей запобігає пропуску критичних вразливостей, емоційний інтелект підтримує конструктивну взаємодію в стресових ситуаціях, проактивність сприяє ініціативному пошуку вразливостей і пропозиції покращень.

Висновки

М'які навички є невід'ємною складовою професійної компетентності пентестера, доповнюючи технічні знання та забезпечуючи ефективність у виконанні завдань у сфері кібербезпеки. Проведене дослідження показало, що ключові м'які навички, такі як комунікація, аналітичне мислення, етична поведінка, адаптивність, співпраця та управління часом, є найбільш затребуваними провідними організаціями та відображені у професійних стандартах, таких як ENISA ESCF[6] та EC-Council CEH[7]. Однак аналіз виявив, що вимоги до м'яких навичок можуть варіюватися залежно від специфіки компанії чи проєкту, що ускладнює їх універсальну стандартизацію. У деяких випадках надмірна

узагальненість стандартів може призводити до ігнорування контекстуальних особливостей, тоді як вузька спеціалізація може не враховувати ширший спектр компетенцій. Таким чином, актуальним напрямком подальших досліджень є розробка гнучких моделей компетенцій, які поєднують універсальні м'які навички з адаптованими вимогами до конкретних ролей у сфері кібербезпеки, забезпечуючи їх інтеграцію з технічними навичками.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 10Guards. URL: https://10guards.com/ua/blog/2022/02/21/pentester-the-profession-of-ethical-hacker/ (дата звернення: 13.06.2025).
2. IBM. Пошук вакансій у сфері безпеки. URL: https://www.ibm.com/careers/search?field_keyword_08[0]=Security (дата звернення: 13.06.2025).
3. Sigma Software. URL: https://career.sigma.software/uk/what-we-offer/vacancies/(дата звернення: 13.06.2025).
4. EC-Council Certified Ethical Hacker (CEH). URL: https://www.eccouncil.org/train-certify/certified-ethical-hacker-ceh/#section_course_info (дата звернення: 13.06.2025).
5. DOU. URL: https://dou.ua/ (дата звернення: 13.06.2025).
6. ENISA Cybersecurity Certification Framework. URL: https://www.enisa.europa.eu/topics/product-security-and-certification/cybersecurity-certification-framework (дата звернення: 13.06.2025).
7. PIN-UP Global. URL: https://pin-up.global/vacancy/penetration-testing-specialist-2/ (дата звернення: 13.06.2025).

Гнітецька Діана Олександрівна – студентка групи 1БКС-24б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: canisasjackal@gmail.com

Науковий керівник: ***Баришев Юрій Володимирович*** - к. т. н., доцент, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: yuriy.baryshev@vntu.edu.ua

Diana Hnitetska – student, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: canisasjackal@gmail.com

Supervisor: ***Yurii Baryshev*** – associate professor of the Information Protection Department, Vinnytsia National Technical University, Vinnytsia, e-mail: yuriy.baryshev@vntu.edu.ua