

АНАЛІЗ БАЧЕННЯ ФАХІВЦІВ З ЕТИЧНОГО ХАКІНГУ В ПРОФЕСІЙНИХ СТАНДАРТАХ УКРАЇНИ ТА ЄС

Вінницький національний технічний університет

Анотація

Розглянуто задачу визначення набору навичок, які висуваються до фахівців з кібербезпеки, пов'язаних з етичним хакінгом. Визначено основні стандарти, що регулюють професійні вимоги до фахівців етичного хакінгу. Виконано порівняльний аналіз цих документів. На основі аналізу визначено набір професійних навичок галузі кібербезпеки, які висуваються до фахівців з етичного хакінгу.

Ключові слова: кібербезпека, етичний хакінг, нормативно-правове регулювання, тестування на проникнення, аналіз вразливостей, кібердослідження.

Abstract

The task of determining the set of skills required of cybersecurity professionals related to ethical hacking is considered. The main standards regulating the professional requirements for ethical hacking professionals are determined. A comparative analysis of these documents is performed. Based on the analysis, a set of professional skills in the cybersecurity industry that are required of ethical hacking professionals is determined.

Keywords: cybersecurity, ethical hacking, regulatory documents, penetration testing, vulnerability analysis, cybersecurity research.

Вступ

Підготовка фахівців у Вінницькому національному технічному університеті (ВНТУ) вимагає постійного дослідження навичок, якими повинні володіти випускники. Мінливість понять внаслідок перманентних змін в галузі кібербезпеки та функцій, які виконують фахівці цієї діяльності під час виконання трудових обов'язків, породжує невизначеність для закладів вищої освіти. Ситуація погіршується ще й тим, що бажано, не лише враховувати сучасний стан галузі, але й враховувати тренди змін, адже за час навчання здобувачів освіти ситуація в галузі буде продовжувати змінюватись. Так під час розробки нової освітньо-професійної програми, направленої, на підготовку фахівців з етичного хакінгу у ВНТУ, виникла актуальна задача дослідження сучасного бачення цих фахівців з точки зору нормативно-правового регулювання галузі кібербезпеки.

Метою даного дослідження є покращення стану кібербезпеки у регіоні шляхом ідентифікації основних навичок підготовки фахівців кібербезпеки, які спеціалізуються на етичному хакінгу.

Аналіз нормативно-правової бази

Задача визначення критеріїв аналізу інструментів до етичного хакінгу наразі ускладнена відсутністю уніфікованого тлумачення цього фаху. Так в Україні набір навичок етичного хакера згадується в низці професійних стандартів, з-поміж яких, в першу чергу, це такі:

- аналітик з оцінки вразливостей [1], який покликаний виявляти вразливості в інформаційних системах та мережах підприємств й установ, а також усувати ці вразливості;
- фахівець з тестування систем захисту інформації [2], який зорієнтований на підготовці та проведенні тестування систем кібербезпеки, а також створенні практичних рекомендацій щодо покращення її поточного стану;
- фахівець з кібердосліджень та розробок систем безпеки [3], фокус якого зосереджено на провадженні досліджень, покликаних підтримувати управлінські рішення щодо покращення та розроблення засобів та систем кібербезпеки.

Крім того, в рамці навичок професіоналів з кібербезпеки Європейського Союзу ECSF [4] "етичний хакер" згадується як альтернативна назва до фахівців з тестування на проникнення (penetration tester). Оскільки саме цей документ наразі є єдиним в нормативно-правовому полі, де чітко визначено це формулювання, відповідно його було взято за основу аналізу бачення фахівців з етичного хакінгу з боку органів, що виконують функції юридичного регулювання галузі. В таблиці 1 наведено результа-

ти виконаного аналізу трудових функцій фахівців з етичного хакінгу, які висуваються в цих документах.

Таблиця 1. Результати порівняльного аналізу нормативно-правових документів

Навичка	Нормативний документ			
	Penetration tester ECSF [4]	Аналітик з оцінки вразливостей [1]	Фахівець з тестування систем захисту інформації [2]	Фахівець з кібердосліджень та розробок систем безпеки [3]
1. Виявляти, аналізувати та оцінювати технічні та організаційні вразливості кібербезпеки	+	+	+	+
2. Визначати вектори атак, виявляти та демонструвати використання технічних вразливостей кібербезпеки	+	+	+	+
3. Тестувати системи та операції на відповідність нормативним вимогам	+	+	+	-
4. Обирати і розробляти відповідні методи тестування на проникнення	+	+	+	+
5. Розробляти плани тестування та процедури для тестування на проникнення	+	+	+	-
6. Визначення процедур для аналізу результатів тестування на проникнення та звітності	+	+	+	-
7. Документування та інформування зацікавлених сторін у результатах тестування на проникнення	+	+	+	+
8. Розгортати інструменти тестування на проникнення, а також програм, що тестуються	+	+	+	-
9. Виконувати дослідження фактичних функцій програмного забезпечення	-	-	-	+
10. Виконувати дослідження обізнаності працівників щодо кібербезпеки	-	+/-	-	+
11. Координувати впровадження засобів та заходів покращення кібербезпеки	-	+	+	+
12. Виявляти вразливості "нульового дня"	-	-	-	+

Як видно з таблиці 1 національні стандарти передбачають більше трудових функцій, які має виконувати фахівець, порівняно з більш вузькоспеціалізованими вимогами ЄС. В таблиці позначено як "+/-" стосовно аналітика з оцінки вразливостей щодо завдання "виконувати дослідження обізнаності працівників щодо кібербезпеки", оскільки до його обов'язків входить визначення адекватності покладених на працівника обов'язків щодо реалізації заходів кібербезпеки. Водночас таке формулювання явно поступається за охопленням завданням фахівця з кібердосліджень та розробок систем безпеки, оцінювання якого має враховувати набагато більше факторів, включно із загальною обізнаністю персоналу щодо усвідомлення ризиків і навичок участі у процесах кібербезпеки об'єкта інформаційної діяльності.

Крім того, варто звернути увагу, що формалізація вимог до фахівців з етичного хакінгу в досліджених документах не завжди відповідала критеріям якості вимог таких як однозначність та завершеність. Так в ECSF [4] як навичку фахівця зазначено "Проводити етичний хакінг" без надання більш детального тлумачення цієї функції.

Висновки

Мінливість галузі кібербезпеки породжує невизначеність в тлумаченні певних професій, а також відмінностей, пов'язаних з різним рівнем автоматизації процесів кібербезпеки. Відповідно виникає різне тлумачення вимог до фахівця певного напрямку. Особливої значущості це набуває для професій, які з'явилися нещодавно, зокрема для фахівців з етичного хакінгу.

Отримані результати порівняльного аналізу стандартів професій показали високий ступінь близькості вимог стандартів до фахівця з тестування систем захисту інформації та аналітика з оцінки вразливостей, що дозволяє прогнозувати злиття з плином часу цих напрямів в єдиний фах. Крім того, рамка професій з кібербезпеки ЄС передбачає менше трудових обов'язків, покладених на фахівців, що дозволяє їм набувати глибшої спеціалізації за рахунок втрати універсалізму.

Подальші дослідження в цьому напрямі доцільно спрямувати на порівняння вимог нормативно-правових документів з вимогами ринку праці та баченням фахівців з етичного хакінгу потенційними роботодавцями.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Професійний стандарт. Аналітик з оцінки вразливостей. Затверджено наказом Адміністрації ДССЗІУ 23 січня 2024 року № 38. 26 с. URL: https://register.nqa.gov.ua/uploads/0/565-analitik_z_ocinki_vrazlivostej_v_2.pdf (дата звернення: 21.03.2025).

2. Професійний стандарт. Фахівець з тестування систем захисту інформації. Затверджено наказом Адміністрації ДССЗІУ 23 січня 2024 року № 38. 23 с. URL: https://register.nqa.gov.ua/uploads/0/577-fahivec_z_testuvanna_sistem_zahistu_informacii_v_2.pdf (дата звернення: 21.03.2025).

3. Професійний стандарт. Фахівець з кібердосліджень та розробок систем безпеки. Затверджено наказом Адміністрації ДССЗІУ 23 січня 2024 року № 38. 29 с. URL: https://register.nqa.gov.ua/uploads/0/573-fahivec_z_kiberdoslidzen_ta_rozrobok_sistem_bezpeki_v_2.pdf (дата звернення: 21.03.2025).

4. ENISA. ECSF: European Cybersecurity Skills Framework. 19.09.2022. 27 p. URL: <https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20Role%20Profiles.pdf> (accessed 21.03.2025).

Баришев Юрій Володимирович — канд. техн. наук, доцент кафедри захисту інформації, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: yuriy.baryshev@vntu.edu.ua

Yurii Baryshev — PhD. (Eng), Associate Professor of Information Protection Department, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : yuriy.baryshev@vntu.edu.ua