PYTANIA Z PRZEDMIOTÓW ZWIĄZANYCH Z TEMATYKĄ PRACY DYPLOMOWEJ

1. W jakim stopniu europejski i krajowy program certyfikacji cyberbezpieczeństwa przyczyniają się do podnoszenia poziomu bezpieczeństwa systemów informatycznych oraz jakie ograniczenia praktyczne wiążą się z ich wdrażaniem?
2. Jakie są aktualne wyzwania stojące przed cyberbezpieczeństwem Rzeczypospolitej Polskiej i w jaki sposób wpływają one na funkcjonowanie administracji publicznej, gospodarki oraz bezpieczeństwo obywateli?
3. W jaki sposób przestępcy wykorzystują cyfrowe platformy internetowe do popełniania przestępstw, jakie cechy tych platform sprzyjają działalności przestępczej oraz jak kształtuje się kwalifikacja prawna czynów ukierunkowanych na platformy cyfrowe?
4. Jak zorganizowany jest instytucjonalny system organów ścigania w zakresie zwalczania przestępstw komputerowych i w jakim zakresie kompetencyjnym poszczególne organy realizują swoje zadania?
5. Jakie elementy konstytuują przestępstwo komputerowe określane mianem „hackingu", gdzie zostało ono spenalizowane oraz w jaki sposób jego typowe i kwalifikowane postacie są wykorzystywane w praktyce przestępczej?
6. Jakie rodzaje nieuczciwej reklamy zostały wyróżnione w ustawie o zwalczaniu nieuczciwej konkurencji i w jakim stopniu wybrany typ (np. reklama podprogowa) narusza interesy konsumentów oraz zasady uczciwej konkurencji?
7. Jakie zagrożenia wynikają z cyberprzestępczości oraz funkcjonowania mediów społecznościowych w wymiarze indywidualnym, społecznym i międzynarodowym oraz jakie typy przestępstw są najczęściej popełniane z ich wykorzystaniem?
8. Czym jest OSINT jako metoda pozyskiwania informacji, jakie są jej cele i etapy realizacji oraz w jakim zakresie jej stosowanie jest dopuszczalne w świetle obowiązujących przepisów prawa?
9. Jakie podstawowe kategorie przestępstw komputerowych zostały wyróżnione w Konwencji o cyberprzestępczości i w jaki sposób determinują one kierunki krajowej polityki kryminalnej?
10. Na czym polega odpowiedzialność karna za przestępstwa przeciwko ochronie informacji (tajemnica państwowa, służbowa, zawodowa) realizowane przy użyciu systemów

teleinformatycznych?

11. Jakie znaczenie mają botnety we współczesnej przestępczości komputerowej oraz jakie narzędzia stosują organy ścigania w celu ich identyfikacji i neutralizacji?
12. W jaki sposób realizowane jest ujawnianie i zabezpieczanie śladów cyfrowych pozostawionych w systemach komputerowych i sieciach teleinformatycznych oraz jakie błędy mogą obniżyć wartość dowodową materiału?
13. Jakie są kluczowe etapy pracy biegłego informatyki śledczej oraz jakie pytania powinien formułować organ procesowy, aby ekspertyza miała najwyższą wartość dowodową?
14. Jakie metody ataków socjotechnicznych (np. phishing, pretexting, baiting) są obecnie najskuteczniejsze i jakie mechanizmy ochronne powinien stosować użytkownik oraz instytucja?
15. W jaki sposób struktura i obowiązki krajowego systemu cyberbezpieczeństwa wpływają na efektywność reagowania na incydenty, a jakie bariery ujawniają się w praktyce funkcjonowania KSC?
16. Jak kształtuje się rola ENISA oraz europejskich CSIRT w budowaniu spójnego systemu cyberbezpieczeństwa Unii Europejskiej?
17. Jak analiza mediów społecznościowych może wspierać proces profilowania sprawców oraz identyfikacji zagrożeń dla bezpieczeństwa publicznego?
18. Jakie ograniczenia prawne i techniczne pojawiają się w procesie pozyskiwania danych od dostawców usług cyfrowych w Polsce i w ramach współpracy międzynarodowej?
19. Jakie są główne różnice pomiędzy cyberprzestępczością indywidualną, zorganizowaną i państwową (state-sponsored) oraz jakie wyzwania rodzą one dla organów ścigania?
20. Na czym polega mechanizm ataku ransomware w kontekście jego faz operacyjnych, metod szyfrowania i modeli biznesowych (RaaS), a jakie działania prewencyjne i reakcyjne są najbardziej efektywne?