

93
DECYZJA NR
DYREKTORA BIURA ŁĄCZNOŚCI I INFORMATYKI
KOMENDY GŁÓWNEJ POLICJI

z dnia 06. CZE. 2024 2024 r.

**zmieniająca decyzję w sprawie szczegółowej struktury organizacyjnej i schematu organizacyjnego
Biura Łączności i Informatyki Komendy Głównej Policji, podziału zadań między dyrektorem a jego
zastępcami oraz katalogu zadań komórek organizacyjnych**

Na podstawie § 12 ust. 1 zarządzenia nr 2 Komendanta Głównego Policji z dnia 1 kwietnia 2016 r. w sprawie regulaminu Komendy Głównej Policji (Dz. Urz. KGP poz. 13, z późn. zm.¹⁾) postanawia się, co następuje:

§ 1. W decyzji nr 97 Dyrektora Biura Łączności i Informatyki Komendy Głównej Policji z dnia 27 maja 2020 r. w sprawie szczegółowej struktury organizacyjnej i schematu organizacyjnego Biura Łączności i Informatyki Komendy Głównej Policji, podziału zadań między dyrektorem a jego zastępcami oraz katalogu zadań komórek organizacyjnych, zmienionej decyzją nr 184 z dnia 26 października 2021 r., decyzją nr 40 z dnia 23 marca 2022 r. oraz decyzją nr 80 z dnia 12 maja 2023 r. wprowadza się następujące zmiany:

1) w § 1 w ust. 1 pkt 4 otrzymuje brzmienie:

„4) Wydział Cyberbezpieczeństwa, w skład którego wchodzi Sekcja do spraw Utrzymania Centralnych Systemów Internetowych i Obsługi Incydentów Cyberbezpieczeństwa w Poznaniu;”;

2) § 8 otrzymuje brzmienie:

„§ 8. 1. Do zadań Wydziału Cyberbezpieczeństwa należy w szczególności:

- 1) rozpoznawanie w sieci Internet oraz sieciach i systemach Policji zagrożeń cyberbezpieczeństwa mających wpływ na cyberbezpieczeństwo w Policji;
- 2) inicjowanie i wspieranie działań komórek organizacyjnych KGP oraz jednostek organizacyjnych Policji w obszarze osiągnięcia zdolności do zapewnienia bezpieczeństwa cyberprzestrzeni Policji;
- 3) zaawansowana obsługa incydentów cyberbezpieczeństwa w jawnych systemach i sieciach teleinformatycznych Policji;
- 4) koordynowanie obsługi zgłoszonych incydentów cyberbezpieczeństwa;
- 5) realizowanie zadań związanych z wymianą informacji w ramach Punktu Kontaktowego do spraw ataków na systemy teleinformatyczne;
- 6) administrowanie Centralnymi Systemami Internetowymi i usługami informatycznymi świadczonymi w ramach Centralnego Węzła Internetowego KGP;
- 7) koordynowanie zadań związanych z eksploatacją Centralnych Systemów Internetowych Policji;
- 8) współpraca z zespołami serwisowymi podmiotów zewnętrznych;
- 9) udział w pracach zespołów i grup eksperckich w zakresie właściwości wydziału;
- 10) opracowywanie i przekazywanie rekomendacji w zakresie działań podnoszących poziom cyberbezpieczeństwa w Policji;
- 11) prowadzenie działań w zakresie analizy i przygotowywania zaleceń mających na celu zapobieganie występowania incydentów cyberbezpieczeństwa;
- 12) współpraca z komórkami organizacyjnymi KGP oraz jednostkami organizacyjnymi Policji w zakresie kreowania spójnego, jednolitego i efektywnego systemu zarządzania bezpieczeństwem cyberprzestrzeni Policji;
- 13) wnioskowanie do właściwej komórki organizacyjnej KGP lub jednostki organizacyjnej Policji w sprawie czasowego wyłączenia lub zaniechania przetwarzania informacji w systemie lub sieci

¹⁾Zmiany wymienionego zarządzenia zostały ogłoszone w Dz. Urz. KGP z 2016 r. poz. 69, z 2017 r. poz. 44, z 2018 r. poz. 2, 106, i 126, z 2019 r. poz. 105 i 126, z 2020 r. poz. 16, z 2021 r. poz. 15, 57 i 101, z 2022 r. poz. 88, 199 i 218, z 2023 r. poz. 7, 40 i 79 oraz z 2024 r. poz. 11.

- teleinformatycznej Policji w związku z wystąpieniem incydentu cyberbezpieczeństwa;
- 14) projektowanie, testowanie, wdrażanie oraz opiniowanie nowych rozwiązań technicznych dla utrzymania odpowiedniego poziomu bezpieczeństwa komunikacji elektronicznej Policji;
 - 15) administrowanie krajowym węzłem dostępu do sieci 1-24/7 INTERPOL;
 - 16) wspieranie Zespołu POL-CERT w realizowaniu zadań;
 - 17) opracowywanie i wdrażanie Policyjnych Standardów Cyberbezpieczeństwa w CSI oraz promowanie dobrych praktyk i zaleceń;
 - 18) prowadzenie testów penetracyjnych i audytów cyberbezpieczeństwa sieci i systemów teleinformatycznych Policji;
 - 19) współpraca krajowa i międzynarodowa w zakresie cyberbezpieczeństwa na poziomie technicznym z podmiotami sektora rządowego państw Unii Europejskiej, Stanów Zjednoczonych Ameryki Północnej oraz Organizacją Traktatu Północnoatlantyckiego;
 - 20) współpraca z podmiotami pozapolicyjnymi w zakresie upowszechniania wiedzy nt. cyberbezpieczeństwa;
 - 21) współpraca i wymiana informacji w zakresie zwalczania cyberprzestępczości z właściwymi komórkami organizacyjnymi KGP oraz jednostkami organizacyjnymi Policji;
 - 22) aktywne poszukiwanie zagrożeń cyberbezpieczeństwa (CyberThreat Intelligence i ThreatHunting);
 - 23) analizowanie złośliwego oprogramowania;
 - 24) badanie bezpieczeństwa, podatności i testowanie sprzętu lub oprogramowania;
 - 25) ocena bezpieczeństwa systemów informacyjnych, w tym przeprowadzanie testów penetracyjnych i audytów bezpieczeństwa;
 - 26) prowadzenie specjalistycznych analiz cyberbezpieczeństwa i wykrywanie nowych podatności,
 - 27) rozwijanie specjalistycznych narzędzi technicznych wspomagających realizację zadań z zakresu cyberbezpieczeństwa;
 - 28) prowadzenie działań prewencyjnych zwiększających cyberbezpieczeństwo;
 - 29) przyjmowanie zgłoszeń i obsługa incydentów poważnych;
 - 30) wstępna obsługa incydentów cyberbezpieczeństwa;
 - 31) reagowanie na incydenty cyberbezpieczeństwa oraz ich klasyfikacja;
 - 32) prowadzenie zaawansowanych działań z zakresu aktywnej obrony systemów informacyjnych;
 - 33) korelacja danych oraz prowadzenie analiz cyberbezpieczeństwa;
 - 34) nadawanie i weryfikowanie uprawnień użytkowników w ramach usług świadczonych przez Centralne Systemy Internetowe Policji oraz Centralny Węzeł Internetowy KGP;
 - 35) prowadzenie akcji podnoszących świadomość w obszarze cyberbezpieczeństwa, w tym organizacja szkoleń;
 - 36) szacowanie ryzyka w obszarze cyberbezpieczeństwa w Policji.

2. Do zadań Sekcji do spraw Utrzymania Centralnych Systemów Internetowych i Obsługi Incydentów Cyberbezpieczeństwa w Poznaniu należy w szczególności:

- 1) monitorowanie wydajności, obciążenia i przepustowości infrastruktury teleinformatycznej oraz podejmowanie działań modernizacyjnych w zakresie infrastruktury teleinformatycznej w celu optymalnego wykorzystania posiadanych zasobów;
- 2) przeprowadzanie analiz funkcjonujących usług pod kątem ich optymalizacji;
- 3) zgłaszanie potrzeb i propozycji w zakresie optymalizacji procesów przetwarzania danych w systemach informatycznych utrzymywanych przez wydział;
- 4) dokonywanie niezbędnych modyfikacji instrukcji i procedur dotyczących bezpieczeństwa informacji w celu zapewnienia zgodnego z założeniami i sprawnego działania systemów informatycznych pozostających we właściwości wydziału;
- 5) powiadamianie interesariuszy o awariach oraz wszelkich zaobserwowanych nieprawidłowościach w funkcjonowaniu systemów informatycznych;

- 6) współpraca z zespołami serwisowymi podmiotów zewnętrznych w celu jak najszybszego usunięcia zgłoszonych nieprawidłowości i awarii;
 - 7) wymiana informacji w ramach punktów kontaktowych Zespołu POL-CERT;
 - 8) całodobowy monitoring i obsługa systemów bezpieczeństwa Centralnego Węzła Internetowego KGP;
 - 9) wspieranie użytkowników w zakresie dostępu do usług;
 - 10) techniczne zarządzanie od strony administracyjnej uprawnieniami użytkowników Centralnego Węzła Internetowego KGP w zakresie dostępu mobilnego i niestandardowych usług;
 - 11) koordynowanie, inicjowanie i uruchamianie procedur reagowania na incydenty cyberbezpieczeństwa w jawnych systemach i sieciach teleinformatycznych Policji;
 - 12) zabezpieczanie i zlecanie zabezpieczenia śladów cyfrowych związanych z incydentami cyberbezpieczeństwa;
 - 13) opracowywanie wytycznych i standardów w zakresie architektury bezpieczeństwa systemów teleinformatycznych Policji;
 - 14) wspieranie działań komórek organizacyjnych KGP oraz jednostek organizacyjnych Policji, w szczególności Komendy Wojewódzkiej Policji w Poznaniu, w obszarze osiągania zdolności do zapewnienia bezpieczeństwa cyberprzestrzeni Policji;
 - 15) stosowanie zaakceptowanych środków technicznych i organizacyjnych do zdalnego zarządzania i kontroli konfiguracji sieci i systemów teleinformatycznych;
 - 16) prowadzenie portali informacyjnych na potrzeby obsługi incydentów cyberbezpieczeństwa dla jawnych systemów i sieci teleinformatycznych Policji;
 - 17) organizowanie szkoleń z zakresu reagowania na incydenty cyberbezpieczeństwa;
 - 18) udzielanie opinii dotyczącej nowych projektów teleinformatycznych Policji w zakresie cyberbezpieczeństwa;
 - 19) analiza i zarządzanie w zakresie reagowania na wykryte podatności sprzętu i oprogramowania;
 - 20) specjalistyczne zadania realizowane w ramach SOC lub Centrum Zarządzania Siecią (NOC) obejmujące monitoring bezpieczeństwa (analiza i korelacja logów), identyfikację i wstępną obsługę incydentów.”;
- 3) załącznik do decyzji otrzymuje brzmienie określone w załączniku do niniejszej decyzji.

§ 2. Decyzja wchodzi w życie z dniem 15 czerwca 2024 r.

DYREKTOR
BIURA ŁĄCZNOŚCI I INFORMATYKI
KOMENDY GŁÓWNEJ POLICJI

insp. Przemysław WJĘCŁAII

Uzasadnienie

Zmiana decyzji nr 97 Dyrektora Biura Łączności i Informatyki Komendy Głównej Policji z dnia 27 maja 2020 r. w sprawie szczegółowej struktury organizacyjnej i schematu organizacyjnego Biura Łączności i Informatyki Komendy Głównej Policji, podziału zadań między dyrektorem a jego zastępcami oraz katalogu zadań komórek organizacyjnych, zmienionej decyzją nr 184 z dnia 26 października 2021 r., decyzją nr 40 z dnia 23 marca 2022 r. oraz decyzją nr 80 z dnia 12 maja 2023 r., wynika z zatwierdzonej przez Komendanta Głównego Policji notatki służbowej, dotyczącej wzmocnienia etatowego Biura Łączności i Informatyki KGP, którego głównym celem jest zagwarantowanie sprawnej i efektywnej realizacji zadań, przede wszystkim poprzez optymalizację struktury biura oraz racjonalnego wykorzystania pozyskanych zasobów kadrowych.

Powyższe polega na utworzeniu w Wydziale Cyberbezpieczeństwa Sekcji do spraw Utrzymania Centralnych Systemów Internetowych i Obsługi Incydentów Cyberbezpieczeństwa w Poznaniu oraz zapewnieniu ciągłości kierowania i sprawowania nadzoru w ww. Sekcji.

SCHEMAT ORGANIZACYJNY BIURA ŁĄCZNOŚCI I INFORMATYKI KOMENDY GŁÓWNEJ POLICJI

