NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie

LSZ – 4101-26-04/2012
P/12/096

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie
ul. Jacka Odrowąża 1, 71-420 Szczecin
T +48 91 831 39 00, F +48 91 831 39 66
lsz@nik.gov.pl

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli

P/12/096 – Planowanie i realizacja wybranych projektów teleinformatycznych, mających na celu usprawnienie funkcjonowania jednostek organizacyjnych Policji.

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Delegatura w Szczecinie

Kontrolerzy

Maciej Mikulski, specjalista kontroli państwowej, upoważnienie do kontroli nr 85158 z dnia 19.11.2012 r.

Krzysztof Szczepaniak, specjalista kontroli państwowej, upoważnienie do kontroli nr 85177 z dnia 3.01.2013 r.

(dowód: akta kontroli str. 1-4)

Jednostka kontrolowana

Komenda Miejska Policji w Koszalinie ul. Słowackiego 11, 75-009 Koszalin[1].

Kierownik jednostki kontrolowanej

Wiesław Tyl – Komendant Miejski Policji w Koszalinie[2].

(dowód: akta kontroli str. 5-6)

II. Ocena kontrolowanej działalności

1. System Wspomagania Dowodzenia[3].

Ocena ogólna

Najwyższa Izba Kontroli pozytywnie[4] ocenia działalność KMP w zakresie realizacji i wdrożenia projektu teleinformatycznego SWD.

Uzasadnienie oceny ogólnej

Wyniki kontroli wykazały, że SWD jest podstawowym narzędziem pracy służby dyżurnej w KMP. W systemie są rejestrowane wszystkie wymagające tego zgłoszenia, zdarzenia oraz czynności związane z reakcją Policji. Na bieżąco wprowadzana jest dyslokacja służb patrolowo-interwencyjnych oraz zespołów dochodzeniowo-śledczych. Stwierdzono, że urządzenia i sprzęt komputerowy otrzymane do obsługi SWD są wykorzystywane w sposób zgodny z przeznaczeniem.

2. E-Posterunek.

Ocena ogólna

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, działania podejmowane przez KMP w zakresie realizacji i wdrażania projektu teleinformatycznego e-Posterunek.

Uzasadnienie oceny ogólnej

Wyniki kontroli wykazały, że aplikacja e-Posterunek nie została do końca 2012 r. wdrożona w Komendzie i nie była wykorzystana do prowadzenia postępowań przygotowawczych. Komendant nie miał wpływu na określenie terminu wdrożenia aplikacji. KMP nie otrzymała wytycznych w tym zakresie od jednostek organizacyjnych wyższego szczebla, tj. od Komendy Wojewódzkiej Policji

[1] Zwana dalej „KMP" lub „Komendą".
[2] Zwana dalej „Komendantem" lub „Komendantem KMP".
[3] Zwany dalej „SWD".
[4] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.

w Szczecinie[5] i Komendy Głównej Policji[6]. W dniu 21.12.2012 r. KMP została poinformowana przez KWP, o wstrzymaniu wykorzystywania aplikacji do prowadzenia postępowań przygotowawczych na rzeczywistych danych.

Stwierdzone nieprawidłowości dotyczyły w szczególności:

- przekazywania ze zwłoką otrzymanego sprzętu na potrzeby obsługi e-Posterunku,
- niewykorzystania urządzenia mobilnego, przekazanego do użytkowania pracownikowi Wydziału dw. z Korupcją i Przestępstwami Gospodarczymi[7] KMP,
- niestosowania zabezpieczeń technicznych wymaganych na podstawie art. 36 ust. 1 ustawy o ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[8], załącznika do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.[9], a także wewnętrznych regulacji Policji.

III. Opis ustalonego stanu faktycznego

1. Realizacja w KMP projektów teleinformatycznych dotyczących SWD i e-Posterunku.

1.1. SWD.

Opis stanu faktycznego

W KMP nie opracowano żadnych wewnętrznych aktów prawnych ani procedur dotyczących zasad organizacji pracy komórek organizacyjnych Komendy z wykorzystaniem systemu SWD. Z udzielonych wyjaśnień wynika, że wdrożenie ww. systemu realizowano w oparciu o istniejące struktury i obowiązujące zasady funkcjonowania jednostek i komórek organizacyjnych i nie wymagało podjęcia odrębnych działań organizacyjnych.

(dowód: akta kontroli str. 7-8)

Zarządzeniem nr 453 z dnia 27.04.2011 r. w sprawie form i metod przetwarzania informacji wspomagających kierowanie niektórymi działaniami Policji podejmowanymi w celu wykonania zadań statutowych[10] Komendant Główny Policji zatwierdził terminy wdrożenia SWD. Zgodnie z § 10 ust. 1 pkt 2 ww. zarządzenia nadzór nad funkcjonowaniem SWD w zakresie technicznym, bezpieczeństwa teleinformatycznego, jakości, terminowości i aktualności informacji wprowadzanych do SWD oraz przeszkolenia użytkowników systemu z jego obsługi w terenowych jednostkach organizacyjnych Policji sprawują kierownicy tych jednostek.

(dowód: akta kontroli str. 9-17)

Pismem z 20.09.2011 r.[11] KWP przesłała zatwierdzony „Program doskonalenia zawodowego z zakresu umiejętności podstawowej obsługi SWD funkcjonariuszy garnizonu zachodniopomorskiego".

(dowód: akta kontroli str. 54-62)

Decyzją nr 318/11 z 21.11.2011 r. Komendant Wojewódzki Policji w Szczecinie wyznaczył termin wdrożenia SWD w KMP do dnia 5.12 2011 r.

(dowód: akta kontroli str. 63-67)

---

[5] Zwana dalej „KWP".
[6] Zwana dalej „KGP".
[7] Zwany dalej „WKiPG"
[8] Dz. U. z 2002 r. Nr 101, poz. 926 ze zm., zwana dalej: *ustawą o ochronie danych osobowych*.
[9] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), zwane dalej *rozporządzeniem MSWiA z dnia 29 kwietnia 2004 r.*
[10] Dz. Urz. KGP Nr 4 poz. 27 ze zm.
[11] Znak WS-0400-941/11.

Decyzją nr 19/2012 z 13.03.2012 r. Komendant, zgodnie z wymogami decyzji Komendanta Wojewódzkiego z dnia 21.11.2011 r., wyznaczył lokalnych administratorów SWD w KMP (lokalnego administratora technicznego oraz lokalnego administratora merytorycznego).

(dowód: akta kontroli str. 68)

W okresie objętym kontrolą KMP, na wniosek KWP, dokonała dwóch analiz potrzeb sprzętowych do wdrożenia w jednostce SWD, które dotyczyły:
- dwumonitorowych stanowisk dostępowych dla służby dyżurnej (w styczniu 2010 r. wnioskowano o instalacje jednego stanowiska dostępowego),
- stacji dostępowych dedykowanych na potrzeby SWD (w maju 2012 roku Komendant KMP wskazał na potrzebę doposażenia KMP w 12 komputerów).

Wraz z wnioskiem o analizę potrzeb sprzętowych w 2010 roku zwrócono się do KMP o uwagi przydatne w pełnym wdrożeniu SWD. Na tym jednak etapie udzielenie uwag nie było możliwe, gdyż Komenda nie korzystała jeszcze z aplikacji.

(dowód: akta kontroli str. 69-72)

W dniu 28.11.2008 r. KMP otrzymała 4 zestawy komputerowe (komputer, czytnik kart mikroprocesorowych, dwa monitory LCD, drukarka laserowa), oraz 6 zestawów (komputer, czytnik kart, monitor, drukarka) dedykowane do pracy z systemem SWD. W lutym 2009 r. ww. sprzęt był przekazany na stanowiska: Wydziału Prewencji KMP[12] (stanowiska dyżurne) – 3 szt., Komisariatu I – 3 szt., Komisariatu II - 3 szt., Posterunku w Mielnie – 1 szt.
W latach 2008-2012 KMP nie otrzymała więcej sprzętu z przeznaczeniem do użytkowania SWD.

(dowód: akta kontroli str. 73-76)

W okresie od grudnia 2011 r. do stycznia 2012 r. KMP 3-krotnie dokonywała zgłoszeń dotyczących usterek w funkcjonowaniu SWD drogą elektroniczną.

(dowód: akta kontroli str. 77-78)

Z wyjaśnień Komendanta KMP wynika, że zgłaszanie usterek do ww. systemu w trakcie jego wdrażania odbywało się wszystkimi możliwymi kanałami komunikacyjnymi tj. telefonicznie, pocztą elektroniczną, poprzez nieistniejący już system zgłaszania usterek HelpDesk, Internetowe forum policyjne funkcjonujące w sieci Policyjną Sieć Transmisji Danych[13], Policyjną Platformę Wdrożeniową, faxem i pocztą resortową. SWD umożliwiał pracę w trybie tzw. diagnostycznym, generując plik z błędami, które można wygenerować i wysłać do technologów KGP[14] oraz do Sztabu Policji KWP w Szczecinie.

(dowód: akta kontroli str. 7-8)

W KMP dokonano modernizacji jednej jednostki komputerowej będącej w posiadaniu Wydziału Ruchu Drogowego[15], poprzez rozbudowę pamięci RAM celem usprawnienia pracy w systemie SWD. Rozbudowano zestaw komputerowy Optimus[16], który posiadał w fabrycznej konfiguracji 256 MB pamięci RAM.

(dowód: akta kontroli str. 79-82)

Pierwsza instalacja oprogramowania SWD została przeprowadzona w KMP 7.09.2011 r. na komputerze zainstalowanym na stanowisku pracy lokalnego

[12] Dalej „WP".
[13] Dalej „PSTD"
[14] Za pośrednictwem adresu technologia@policja.gov.pl.
[15] Dalej „WRD"
[16] Model Prestige s/n 400.014.230

administratora technicznego oraz w listopadzie 2011 r. (na 15 komputerach) przez pracowników Zespół Łączności i Informatyki KMP[17]. Instalacja aplikacji na kolejnych stanowiskach dostępowych była dokonywana sukcesywnie w okresie od grudnia 2011 r. do września 2012 r. Aktualizacja aplikacji odbywa się w sposób zdalny przez PSTD. Wg stanu na dzień 31 grudnia 2012 r. aplikacja SWD została zainstalowana na 25 stacjach dostępowych w następujących komórkach organizacyjnych KMP: WP[18] – 9 komputerów, WRD[19] - 4 komputery, ZŁI - 1 komputer oraz komisariatach: Komisariacie I Policji[20] – 5 komputerów, Komisariacie II Policji[21] – 6 komputerów.

(dowód: akta kontroli str. 83-87)

System został zainstalowany na 7 z 10 otrzymanych w 2008 r. zestawów stacji dostępowych przeznaczonych w pierwszej kolejności do obsługi SWD i innych policyjnych systemów teleinformatycznych oraz 18 stacjach dostępowych przygotowanych przez pracowników ZŁI w związku z wdrażaniem SWD.

(dowód: akta kontroli str. 73-76, 83-87, 99-101)

Na 3 z 10 otrzymanych ww. stacji dostępowych przeznaczonych m.in. do obsługi SWD, tj. zestawów komputerów stacjonarnych Optimus Optitech DB400 ES[22], nie zainstalowano systemu.

(dowód: akta kontroli str. 73-76, 83-87, 99-101)

Komendant wyjaśnił, że na 3 spośród 10 komputerów na dzień dzisiejszy zakres wykonywanych zadań nie wymaga dostępu do aplikacji SWD. W związku z tym, iż sprzęt komputerowy podłączony jest do PSTD i wykorzystywany do przetwarzania danych osobowych, przygotowywanie jego wymaga wdrożenia obowiązujących wymogów bezpieczeństwa przedstawionych w instrukcjach m.in. „Zalecenia dotyczące standardów technicznych użytkowych oraz bezpieczeństwa, stosowanych w Policji w zakresie informatyki i łączności", „Instrukcja zarządzania systemem informatycznym przetwarzającym dane osobowe Krajowego Systemu Informacyjnego Policji (KSIP)", „Instrukcja administrowania systemem SWD". Sprzęt komputerowy przekazywany jest po wdrożeniu ww. zasad i uzgodnieniu z użytkownikami końcowymi dogodnego terminu jego przekazania niezwłocznie celem sprawnej realizacji zadań służbowych.

(dowód: akta kontroli str. 79-82)

Na dzień 31 grudnia 2012 r. według elektronicznej ewidencji osób upoważnionych do dostępu do SWD, 85 funkcjonariuszy posiadało uprawnienia dostępu do SWD. Na stanowiskach pracy wyposażonych w sprzęt z zainstalowanym SWD (27 w KMP[23], 11 w Komisariacie I i 11 w Komisariacie II), pracowało 49 (z 85) funkcjonariuszy, z czego 28 na stanowiskach służby dyżurnej.

(dowód: akta kontroli str. 83-96)

Jak wyjaśnił Komendant różnica między liczbą osób uprawnionych, a liczbą użytkowników systemu wynika z faktu, że część osób pracuje na jednym i tym samym stanowisku roboczym (przede wszystkim służby dyżurnej), dodatkowo część osób stanowi rezerwę kadrową na ww. stanowisku pracy, koniecznym jest więc posiadanie uprawnień przez te osoby.

---

[17] Zwany dalej „ZŁI"

[18] Naczelnik, Zastępca Naczelnika, Sztab, Zespół Dyżurnych, Zespół ds. Nieletnich.

[19] Naczelnik, zastępca Naczelnika, Odprawiający.

[20] Naczelnik Wydziału Prewencji, Zespół Dyżurnych, Kierownik Ogniwa Patrolowo-Interwencyjnego, Posterunek Policji w Mielnie, Posterunek Policji w Sianowie.

[21] Naczelnik Wydziału Prewencji, Zespół Dyżurnych, Kierownik Ogniwa Patrolowo-Interwencyjnego Posterunek Policji w Bobolicach, Posterunek Policji w Polanowie.

[22] Z czytnikami kart mikroprocesorowymi, monitorami LCD i drukarkami laserowymi, o numerach seryjnych 802.024.048, 802.024.070, 802.024.091. Ww. sprzęt przekazano do użytkowania dzielnicowym z Komisariatu I i Komisariatu II oraz do Zespołu ds. Wykroczeń Wydziału Prewencji Komisariatu I.

[23] 22 - w Wydziale Prewencji KMP, 4 w Wydziale Ruchu Drogowego KMP, 1 – w ZŁI.

(dowód: akta kontroli str. 79-82)

Spośród ww. 85 pracowników, 67 zostało przeszkolonych z obsługi SWD. Szkolenia były przeprowadzane w okresie:
- od lipca do listopada 2011 roku przez: Ośrodek Szkolenia Policji w Łodzi z siedzibą w Sieradzu (przeszkolenie 2 trenerów SWD), Biuro Łączności i Informatyki KGP w Warszawie (dla lokalnego administratora technicznego SWD), KWP (przeszkolenie lokalnego administratora merytorycznego i trenerów SWD),
- od 3 listopada do 8 grudnia 2011 r. - przez trenerów SWD z KWP i KMP (użytkownicy w zakresie wdrożenia SWD) w grupach 6-13 osobowych w wymiarze po 8 godzin i w grupach 1-8 osobowych w wymiarze po 2 godziny.
- od 5 stycznia do 29 października 2012 r. przez trenerów SWD z KMP (użytkownicy w zakresie funkcjonowania SWD) w grupach 1-8 osobowych w wymiarze po 2 godziny.
- we wrześniu 2012 r. – przeszkolenie przez Biuro Łączności i Informatyki KGP - trenerzy SWD (Moduł SDI oraz szkolenie trenerów typu 2).

(dowód: akta kontroli str. 97-98)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

Uwagi dotyczące badanej działalności

1. Spośród 85 pracowników, którzy posiadali uprawnienia do użytkowania SWD, 18 (21,2%) nie zostało przeszkolonych z obsługi tego systemu. Zostali oni wyposażeni jedynie w plik multimedialny, dotyczący działania SWD.

(dowód: akta kontroli str. 88-98, 104)

Komendant wyjaśnił: *18 osób nie zostało przeszkolonych podczas szkoleń kaskadowych, gdyż uprawnienia do SWD nadane im zostały w późniejszym terminie. Ponadto każdy z policjantów zapoznając się z przepisami ustawy o ochronie danych osobowych z dnia 29.08.1997 r. oraz wewnętrznymi aktami prawnymi i dokumentami dotyczącymi ochrony danych osobowych otrzymywał w wersji elektronicznej plik z multimedialnym szkoleniem. Jednocześnie informuję, iż żaden dokument nie określa w jakiej formie powinno być prowadzone szkolenie w związku z czym, powyższą przyjętą przez nas formę należy uznać za prawidłową*

(dowód: akta kontroli str. 79-82)

Z przeprowadzonych w KMP anonimowych ankiet użytkowników końcowych aplikacji SWD wynika, że dla 47% (18 ankietowanych) poziom szkoleń, a także ich ilość nie była wystarczająca do pracy przy obsłudze tego systemu.

(dowód: akta kontroli str. 433-510)

2. SWD nie został zainstalowany na stanowiskach Wydziału Kryminalnego[24] KMP i WKiPG i nie jest użytkowany przez pracowników ww. komórek, pomimo przyznania im uprawnień do ww. systemu.

(dowód: akta kontroli str. 83-87)

Komendant wyjaśnił, że m.in. że wymagania sprzętowe SWD uniemożliwiają lub utrudniają instalację i pracę na przestarzałym sprzęcie komputerowym. Aktualnie planowana jest instalacja przedmiotowej aplikacji na użytkowanym sprzęcie w WK.

(dowód: akta kontroli str. 102-103)

Ocena cząstkowa

Najwyższa Izba Kontroli pozytywnie ocenia działalność KMP w zbadanym zakresie.

[24] Zwany dalej „WK"

1.2. E-Posterunek

Opis stanu faktycznego

W KMP nie opracowano żadnych wewnętrznych aktów prawnych ani procedur dotyczących zasad organizacji pracy komórek organizacyjnych Komendy z wykorzystaniem systemu e-Posterunek. Z udzielonych wyjaśnień wynika, że wdrożenie ww. systemu realizowano w oparciu o istniejące struktury i obowiązujące zasady funkcjonowania jednostek i komórek organizacyjnych i nie wymagało to podjęcia odrębnych działań organizacyjnych. Komendant nie określił terminu wdrożenia ww. systemu.

(dowód: akta kontroli str. 7-8)

Komendant wyznaczył administratorów lokalnych odpowiedzialnych za wdrożenia e-Posterunku (pracowników ZŁI).

(dowód: akta kontroli str. 105)

We wrześniu i październiku 2010 r. oraz styczniu i listopadzie 2011 r., Komendant na wniosek KWP informował o posiadanym sprzęcie komputerowym spełniającym wymogi systemu e-Posterunek. Jednocześnie KMP zgłaszała zapotrzebowanie na 25 jednostek sprzętu dla służb dochodzeniowo-śledczych oraz 36 jednostek dla komórek do spraw dzielnicowych.

(dowód: akta kontroli str.106-118)

W celu obsługi aplikacji e-Posterunek, Komenda otrzymała z KWP łącznie 13 zestawów (komputery stacjonarne, czytniki kart i monitory LCD), 29 komputerów przenośnych (23 urządzenia Notebook Lenovo oraz 6 urządzeń mobilnych Twinhead Durabook U12C) i 3 drukarki mobilne. Sprzęt elektroniczny został dostarczony do KMP w 5 transzach w okresie od maja 2011 r. do listopada 2012 r. Sprzęt komputerowy otrzymany na potrzeby aplikacji e-Posterunek został przekazany do poszczególnych komórek organizacyjnych KMP w terminie: 28 dni (2 drukarki mobilne), 55 dni (13 notebooków), 70 dni (12 stacji dostępowych stacjonarnych), 100 dni (10 notebooków), 170 dni (1 drukarka) oraz 243 dni (6 urządzeń mobilnych) od daty otrzymania sprzętu.

(dowód: akta kontroli str. 119-143)

Komendant wyjaśnił, że otrzymane w okresie od września do grudnia 2011 r. komputery stacjonarne i laptopy w *związku z prowadzonymi szkoleniami w KMP*[25] *w Koszalinie (na rzecz naszej jednostki i pozostałych jednostek garnizonu zachodniopomorskiego) z systemu SWD i brakiem dedykowanej salki szkoleniowej ze sprzętem przeznaczonym tylko w tym celu w uzgodnieniu z KWP zabezpieczono w naszej jednostce na czas szkoleń sprzęt komputerowy, który docelowo został przeznaczony do pracy w naszej jednostce w postaci notebooków Lenovo i komputerów stacjonarnych Topadvert. Szkolenia przeprowadzane były w różnych terminach i przez różny okres czasu, koniecznym więc było zabezpieczenie jednego i drugiego rodzaju sprzętu. Po przeprowadzonych zajęciach sprzęt został przygotowany do eksploatacji we właściwych komórkach organizacyjnych jednostki i niezwłocznie przekazany.*

(dowód: akta kontroli str. 79-82)

W marcu 2011 r. KWP informowała Komendanta KMP o sposobie komunikowania, o sugestiach rozbudowy aplikacji, a także o przekazywaniu opinii policjantów o aplikacji. KMP otrzymała z KWP instrukcje aktualizacji aplikacji oraz algorytm zgłaszania błędów. Z instrukcjami zapoznano administratorów lokalnych oraz potencjalnych użytkowników e-Posterunku z WK, WKiPG, Komisariatów I i II.

(dowód: akta kontroli str. 144-168)

[25] Ww. szkolenia odbyły się w okresie od 3 listopada do 8 grudnia 2011 r. oraz od 5 stycznia do 29 października 2012 r, co opisano w punkcie 1.1 wystąpienia.

W lutym i sierpniu 2011 r. KWP zwróciła się do KMP z prośbą o udzielenie informacji na temat postępów wdrożenia aplikacji e-Posterunek i ilości postepowań przygotowawczych sporządzonych przy jej wykorzystaniu. Z udzielonych odpowiedzi wynikało, że KMP nie przeprowadzała postępowań przy pomocy systemu ze względu na problemy z zapewnieniem wymagań sprzętowych i błędy podczas instalacji aktualizacji systemu. Sygnalizowano błędy w bazie prawnej aplikacji e-Posterunek, brak jej funkcjonalności oraz niedostosowanie systemu do wymogów kodeksu postępowania karnego.

(dowód: akta kontroli str. 167-191)

Docelowymi użytkownikami systemu e-Posterunek w KMP wg stanu na 31.12.2012 r. było 178 funkcjonariuszy z następujących komórek organizacyjnych KMP i komisariatów:

- 74 pracowników Komendy, tj. 47 funkcjonariuszy z zespołów dochodzeniowo-śledczych, tj. WK[26], WKiPG[27], 10 funkcjonariuszy służby prewencyjnej z WP, 2 z ZŁI oraz 15 zajmujących się obsługą ruchu drogowego z WRD,
- 47 funkcjonariuszy Komisariatu I, w tym 28 z zespołów dochodzeniowo-śledczych, tj. WK[28] oraz 19 służby prewencyjnej z WP, Zespołów ds. Prewencji Posterunków w Mielnie i Sianowie
- 57 funkcjonariuszy Komisariatu II, w tym 30 funkcjonariuszy z zespołów dochodzeniowo-śledczych, tj. WK[29] oraz 27 funkcjonariuszy służby prewencyjnej z WP i Zespołów ds. Prewencji Posterunków w Będzinie, Polanowie, Bobolicach.

(dowód: akta kontroli str. 192-233)

Według stanu na 31.12.2012 r. aplikacja e-Posterunek została zainstalowana na 53 komputerach (w tym na otrzymanych 42 jednostkach, dedykowanych do obsługi e-Posterunku oraz dodatkowo na 11 komputerach stacjonarnych posiadanych przez KMP), z czego 22 komputery były użytkowane przez 24 pracowników KMP oraz 31 komputerów przez pracowników Komisariatu I i II. Z 24 pracowników KMP użytkujących sprzęt z zainstalowanym e-Posterunkiem 3 to pracownicy ZŁI, zajmujący się czynnościami administrowania aplikacji, zaś 21 to pracownicy, wykonujący czynności dochodzeniowo-śledcze z WK, WKiPG oraz WP.
Pierwsze instalacje aplikacji e-Posterunek przeprowadzono w miesiącach październik - listopad 2010 r. na 6 komputerach stacjonarnych (2 w WKiPG i 4 w Komisariacie I). W okresie od czerwca 2011 r. do stycznia 2012 r. przeprowadzono kolejne instalacje ww. aplikacji.

(dowód: akta kontroli str. 234-239)

Informacje o kolejnych wersjach aplikacji e-Posterunek były przekazywane do KMP w formie elektronicznej i papierowej przez Wydział Łączności i Informatyki KWP. Wyznaczeni policjanci, w ramach wykonywanych zadań na bieżąco monitorowali w Centrum Dystrybucji Oprogramowania[30] dostępność publikowanych nowych wersji aplikacji. W dniu 8.05.2012 r. KMP została poinformowana przez KWP o udostępnieniu w CDO aktualnej wersji e-Posterunku 2.0.

(dowód: akta kontroli str. 240-242)

Pismem z dnia 22.06.2012 r. Zastępca Komendanta KMP zobowiązał Komendantów Komisariatów, naczelników wydziałów i kierowników komórek KMP do

[26] Referatu Operacyjno-Rozpoznawczego, Zespołu ds. Poszukiwań i Identyfikacji Osób, Zespołu do Walki z Przestępczością Samochodową, Zespołu do. Walki z Przestępczością Narkotykową, Zespołu Dochodzeniowo-Śledczego.
[27] Zespołu Operacyjno-Rozpoznawczego, Zespołu Dochodzeniowo-Śledczego, Zespołu do. Walki z Korupcją, Zespołu do. Walki z Przestępczością Przeciwko Własności Intelektualnej, Przemysłowej i Komputerowej.
[28] Zespołu Operacyjno-Rozpoznawczego, Zespołu Dochodzeniowo-Śledczego, Zespołów ds. Kryminalnych Posterunków w Sianowie i Mielnie.
[29] Zespołu Operacyjno-Rozpoznawczego, Zespołu Dochodzeniowo-Śledczego i Zespołów ds. Kryminalnych Posterunków w Będzinie, Polanowie, Bobolicach.
[30] Dalej „CDO"

sukcesywnego dostarczania komputerów i terminali przewoźnych eksploatowanych przez służby dochodzeniowo-śledcze oraz WRD celem wykonania ww. aktualizacji.

(dowód: akta kontroli str. 243)

Wg stanu na dzień 31 grudnia 2012 r., aktualna wersja oprogramowania 2.0.8. została zainstalowana na 3 komputerach stacjonarnych użytkowanych w KMP, a wersja 2.0.0.3 na 3 stacjach dostępowych (2 komputery stacjonarne i notebook), przeznaczonych do obsługi tej aplikacji.

(dowód: akta kontroli str. 234-239)

Zgodnie z decyzją Komendanta KMP Komendanci Komisariatów oraz Naczelnicy WK i WKiPG wyznaczyli po jednym funkcjonariuszu, którzy mieli zostać przeszkoleni z obsługi e-Posterunku i być odpowiedzialnymi za przeprowadzenie szkoleń pracowników we własnych jednostkach. Szkoleniem trenerów użytkowników aplikacji e-Posterunek zostało objętych 4 funkcjonariuszy KMP. Szkolenie zostało przeprowadzone przez funkcjonariusza KWP w dniu 5.10.2010 r., tj. przed otrzymaniem przez Komendę sprzętu komputerowego przeznaczonego do obsługi tej aplikacji.

(dowód: akta kontroli str. 97-98, 105)

Z wyjaśnień specjalisty z WKiPG wynika, że *było to szkolenie na aplikacji w fazie testów. Po wdrożeniu e-Posterunku w fazę produkcyjną miało nastąpić dalsze szkolenie, które nie nastąpiło.*

(dowód: akta kontroli str. 349-352)

W okresie od marca 2011 r. do lutego 2012 r. KMP 6-krotnie dokonywała zgłoszeń dotyczących błędów i usterek w funkcjonowaniu e-Posterunku oraz uwag dotyczących jego użytkowania drogą pisemną i elektroniczną.

(dowód: akta kontroli str. 77-78)

Imienne hasło do e-Posterunku posiadało 2 z 21 pracowników, pracujących na sprzęcie z zainstalowaną aplikacją. Pozostałych 19 pracowników posiadało dostęp do e-Posterunku poprzez standardowe konta systemowe utworzone dla „użytkownika testującego”[31].

(dowód: akta kontroli str. 234-239, 367)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

Część sprzętu komputerowego otrzymanego na potrzeby aplikacji e-Posterunek, przekazano do poszczególnych komórek organizacyjnych KMP w terminach: 170 dni (1 drukarka mobilna[32]) i 243 dni (6 urządzeń mobilnych Twinhead Durabook U12C33) od daty otrzymania sprzętu z KWP.

(dowód: akta kontroli str. 119-125, 131, 140-143, 553-561)

Komendant wyjaśnił, że w KMP sprzęt komputerowy *wydawany jest niezwłocznie po jego otrzymaniu, skonfigurowaniu, lub zaprzestaniu jego wykorzystania do innych czynności służbowych w czasie gdy formalnie jest księgowany na stanie Zespołu Łączności i Informatyki KMP w Koszalinie (…) W przypadku urządzeń mobilnych Durabook w związku z brakiem drukarek mobilnych dedykowanych do tych urządzeń i wcześniejszym przydzieleniu imiennym sprzętu, zadecydowano o nie wydawaniu sprzętu do czasu ich uzyskania. W chwili kiedy otrzymano informację o tym iż sprzęt takowy ma dotrzeć do KMP w Koszalinie został on niezwłocznie przekazany do właściwych służb*. Komendant dodał, że *rozbieżność, co do ilości dni*

[31] Z loginem „test1”.

[32] HP Office Jet 100 (nr ser. MY14P510RH) odebrana z KWP 28.09.2011 r. wydana do WK 16.03.2012 r.

[33] O nr ser. SY1101000337, SY1101000567, SY1101000995, SY1101000587, SY1101000913, SY1101000032 odebrane z KWP 26.05.2011 r. – wydane użytkownikom w dniu 24.01.2012 r.

pomiędzy przekazaniem sprzętu przez KWP w Szczecinie, a wydaniem do właściwych jednostek KMP w Koszalinie, wynikać może z różnicy występującej pomiędzy datą wystawienia dokumentów przekazania sprzętu przez KWP w Szczecinie, a właściwą datą odebrania sprzętu z magazynu w KWP ze względu na trudności logistyczne, brak własnego sprzętu transportowego w ZŁI i posiłkowanie się przez służby logistyczne pomocą innych wydziałów KMP.

(dowód: akta kontroli str. 79-82)

Uwagi dotyczące badanej działalności

1. Z przedstawionych dokumentów oraz wyjaśnień pracowników wynika, że jedynie 4 z 53 pracowników KMP i Komisariatów I i II (z tego 23 pracowników Komendy), którym powierzono sprzęt do obsługi e-Posterunku odbyło szkolenia z obsługi aplikacji, z czego jedynie 2 pracowników KMP potrafiło zalogować się do e-Posterunku.

(dowód: akta kontroli str. 97-98, 335-367)

W złożonych wyjaśnieniach Komendant potwierdził, że przeszkolonych zostało jedynie 4 funkcjonariuszy (administratorzy merytoryczni). Szkolenie zostało zorganizowane przez Wydział Dochodzeniowo-Śledczy KWP w Szczecinie, dla KMP i innych jednostek z garnizonu zachodniopolskiego. Komendant nie wyjaśnił jednak przyczyny braku szkoleń pozostałych pracowników KMP.

(dowód: akta kontroli str. 79-82)

2. Na 46 (z 53) komputerach z zainstalowanym e-Posterunkiem, nie dokonano aktualizacji ww. aplikacji do wersji 2.0.0.3 lub 2.0.8. Wersja oprogramowania 2.0.8. została zainstalowana na 3 komputerach stacjonarnych użytkowanych w KMP, a wersja 2.0.0.3 na 3 stacjach dostępowych (2 komputery stacjonarne i notebook), przeznaczonych do obsługi tej aplikacji. Na pozostałych 46 komputerach funkcjonowała wersja 1.8.8.0 lub starsze wersje[34] ww. aplikacji.

(dowód: akta kontroli str. 234-239)

Komendant wyjaśnił m.in., że instalowana aplikacja e-Posterunek aktualna była na dzień, w którym przygotowywano sprzęt dla jednostek, w których miał być on docelowo eksploatowany. Podczas aktualizacji pierwszych wersji aplikacji do wyższych jej wersji występowały błędy niezgodności wersji bazy danych, które uniemożliwiały lub utrudniały jej aktualizację, koniecznym było całkowite odinstalowanie aplikacji włącznie z bazą danych i ponowna instalacja aplikacji bazy danych. Osoby, które posiadały już sprzęt z zainstalowaną starszą wersją aplikacji w momencie uzyskania informacji o pojawieniu się nowej wersji aplikacji i były zainteresowane jej testowaniem zobowiązane zostały do zgłaszania się do ZŁI celem aktualizacji oprogramowania do najświeższej wersji.

(dowód: akta kontroli str. 79-82)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonej nieprawidłowości, działalność KMP w zbadanym zakresie.

2. Wdrożenie w KMP projektów teleinformatycznych dotyczących SWD i e-Posterunku.

2.1. SWD.

Opis stanu faktycznego

Termin oficjalnego wdrożenia SWD w jednostkach organizacyjnych na poziomie KMP został określony na dzień 5.12.2011 r. i termin ten został dotrzymany. System SWD wykorzystywany był w KMP do bieżącej kontroli podległych służb prewencyjnych w szczególności przez kadrę kierowniczą średniego szczebla, która uzyskiwała informacje o siłach i środkach pozostających w dyspozycji dyżurnego

[34] 1.8.5.0 lub 1.8.2.0

jednostki oraz o wydarzeniach zaistniałych na obszarze działania jednostki, pozwalających na natychmiastowe podejmowanie działań wspierających obsługę zdarzenia lub wydanie poleceń korygujących. Skrócone odpisy zapisów o zaistniałych wydarzeniach stanowią podstawę rozliczenia podległych służb przez kierownictwo jednostki, w tym omówienie trafności i zasadności podejmowanych działań. Informacje te wykorzystywane były również w ramach realizowanego we własnym zakresie programu szkoleniowego oraz do analiz na potrzeby postępowań, prowadzonych w oparciu o przepisy o odpowiedzialności dyscyplinarnej policjantów.

(dowód: akta kontroli str. 244-246)

W KMP równolegle z SWD w formie papierowej prowadzona była „Książka przebiegu służby". Obowiązek prowadzenia tego dokumentu wynikał z polecenia Komendanta Wojewódzkiego Policji w Szczecinie[35] i spowodowany był wymogiem potwierdzania przez dyżurnego własnoręcznym podpisem danych, dotyczących przejętej broni i amunicji, które obligatoryjnie należy wpisać do książki przebiegu służby. Ponadto w formie papierowej obok SWD prowadzone były następujące dokumenty: „Książka służby w patrolach, obchodach i na posterunkach, „Książka kontroli służby", „Książka odpraw i rozliczeń służby patrolowej ogniwa patrolowo-interwencyjnego", oraz „Grafiki służby". W formie papierowej sporządzano także konspekty odpraw do służby[36].

(dowód: akta kontroli str. 244-247)

Z wyjaśnień Komendanta wynika, że potrzeba prowadzenia ww. dokumentów wynikała z pragmatyki służby i realizowanych w związku z tym zadań. Nie wszystkie bowiem osoby uprawnione do dokonywania sprawdzenia sposobu pełnienia służby przez dyżurnych posiadają dostęp (uprawnienia) do systemu SWD. Dane zawarte w ww. dokumentach wykorzystywane były w sytuacjach, w których nie ma możliwości skorzystania z systemu SWD, np. miejsca przeprowadzania odpraw służbowych, w których nie ma stanowiska dostępowego do SWD.

(dowód: akta kontroli str. 244-246)

W wyniku oględzin 4 stanowisk SWD – kierowniczych WP i WRD oraz służby dyżurnego i odprawiającego w zakresie sposobu funkcjonowania w KMP SWD ustalono, że:

- z poziomu dyżurnego aktywne były następujące moduły: „zgłoszenia", „służba", „komunikaty", „raporty", „tryb autonomiczny",
- w systemie były ewidencjonowane informacje dotyczące zgłoszeń przyjmowanych przez dyżurnych, zdarzeń i interwencji oraz dane o: dyslokacji służby patrolowej, zarządzanie patrolami, protokoły z odpraw do służb patrolowych,
- z poziomu kierowników i dyżurnych istniała możliwość przekształcenia zdarzenia SWD w wydarzenie KSIP i bezpośredniego przekazania danych miedzy SWD a KSIP,
- istniała możliwość przeprowadzenia z poziomu SWD sprawdzenia (np. osoby, pojazdu, rzeczy) przez System Poszukiwawczy Policji w KSIP;
- nie była aktywna zakładka mapa,
- była możliwość wygenerowania z systemu wszystkich raportów dostępnych w zakładce kreator raportów – zgodnie z zakresem upoważnień,
- nie było możliwości komunikacji z aplikacją e-Posterunek,
- SWD nie został wyposażony w moduł elektronicznej ewidencji dozorów oraz osób zatrzymanych, ww. ewidencja prowadzona była w formie papierowej,
- SWD dawał możliwość wprowadzania informacji o numerze radiostacji patroli,

[35] Pismo l. dz. IK-VII-026-209/2009 z dnia 18 grudnia 2009 r.
[36] Zgodnie z zarządzeniem nr 768 Komendanta Głównego Policji.

- SWD zawiesza się w trakcie pracy, co utrudnia wykonywanie czynności użytkownikom tego systemu.

Oględziny potwierdziły prowadzenie w formie papierowej: książki służby w patrolach, obchodach i na posterunkach (Mp – 2), książki kontroli służby, książka odpraw i rozliczeń służby patrolowej ogniwa patrolowo – interwencyjnego, książki interwencji (na wypadek awarii SWD) oraz grafików służby.

(dowód: akta kontroli str. 248-295)

Wszystkie zdarzenia i interwencje były ewidencjonowane na bieżąco w SWD. Ogólna liczba zdarzeń zarejestrowanych w SWD od momentu uruchomienia wyniosła 25.517 z czego 2.815 zdarzeń z zakresu ruchu drogowego.

(dowód: akta kontroli str. 248-249, 268-269, 276-277, 282-283, 296-300)

Z przeprowadzonych w KMP anonimowych ankiet 38 użytkowników końcowych aplikacji SWD wynika, że:

- 53% (20 funkcjonariuszy) oceniło, że wprowadzenie aplikacji SWD nie przyczyniło się do usprawnienia ich pracy i podniesienia jej wydajności; 42% (16) oceniło, iż wdrożenie SWD usprawniło pracę i podniosło jej wydajność, pozostałe 5% (2) nie wyraziło opinii;
- 76% (29) wskazało, że wdrożenie SWD nie spowodowało zmniejszenia ilości sporządzanej dokumentacji w formie papierowej; 24% (9) oceniło, iż wdrożenie SWD spowodowało zmniejszenie ilości sporządzanej dokumentacji w formie papierowej;
- 55% (21) oceniło, że ilość i jakość sprzętu komputerowego w Komendzie nie jest wystarczająca do obsługi SWD; 45% (17) oceniła, iż ilość i jakość sprzętu komputerowego jest wystarczająca;
- 45% (17) ankietowanych oceniło, że poziom szkoleń, a także ich ilość jest wystarczająca do pracy przy obsłudze SWD; 47% (18) oceniło, że nie jest wystarczająca, zaś 8% (3) nie miało zdania,
- 61% (23) oceniło SWD jako system średni, a odpowiednio, 32% (12) jako system dobry i 5% (2) jako jednoznacznie zły (1 osoba nie wyraziła opinii).

W ankietach, funkcjonariusze KMP, korzystający z SWD wskazywali w szczególności na następujące problemy związane z funkcjonowaniem tej aplikacji:

- mała wydajność i stabilność systemu, słaba przepustowość łączy oraz częste zawieszanie się aplikacji,
- brak możliwości wyszukania archiwalnych zgłoszeń,
- braki w bazie adresowej.

(dowód: akta kontroli str. 433-510)

W KMP na bieżąco prowadzony był monitoring czasu reakcji na zdarzenie (jako jeden z mierników efektywności pracy Policji). Jak wynika z wyjaśnień Komendanta, w przypadku przekroczenia założonej wartości tego miernika ustala i sprawdza się przyczyny zaistnienia takiej sytuacji, a następnie, w zależności od rodzaju ustalonej przyczyny, podejmowane są stosowne działania mające na celu wyeliminowanie przyczyn wydłużenia czasu reakcji.

(dowód: akta kontroli str. 244-246)

Od chwili wprowadzenia SWD czas reakcji uległ skróceniu, w okresie od 1 stycznia do 30 listopada 2011 roku czas reakcji na terenie miasta wynosił 10,09 minuty, a na terenach wiejskich 15,03 minuty. Po wprowadzeniu SWD czas reakcji wynosi odpowiednio: dla terenu miejskiego 6,47 minuty i 11,02 minuty na obszarach miejskich.

(dowód: akta kontroli str. 244-246, 301-302)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki nie stwierdzono nieprawidłowości.

Uwagi dotyczące badanej działalności

W objętych badaniem Wydziałach KMP tj. WRD i WP grafiki służb funkcjonariuszy prowadzone były w edytorze tekstu OpenOffice, co było podstawowym sposobem ich sporządzania. Grafiki były drukowane i następnie zatwierdzane przez Komendanta KMP. Grafiki służb funkcjonariuszy nie były wprowadzane do SWD, pomimo dostępnej funkcji.

(dowód: akta kontroli str. 247-252, 282-283, 294)

Według wyjaśnień Naczelnika WRD oraz zastępcy Naczelnika WP grafik nie był wprowadzany do SWD z powodu zbyt małej funkcjonalności systemu, czasochłonnej formy wprowadzania i częstych aktualizacji.

(dowód: akta kontroli str. 247-249, 282-283)

Ocena cząstkowa

Najwyższa Izba Kontroli pozytywnie ocenia działalność KMP w zbadanym zakresie.

2.2. E-Posterunek

Opis stanu faktycznego

Od terminu pierwszych instalacji e-Posterunku przeprowadzonych w miesiącach październik - listopad 2010 r., aplikacja nie została wdrożona do dnia zakończenia kontroli (tj. 11.01.2013 r.). Pismem z dnia 21.12.2012 r. Zastępca Komendanta Wojewódzkiego poinformował KMP o wstrzymaniu wykorzystywania ww. systemu do prowadzenia postępowań przygotowawczych na rzeczywistych danych[37].

(dowód: akta kontroli str. 244-246, 303)

W wyniku oględzin sposobu funkcjonowania w KMP e-Posterunku i wykorzystania tej aplikacji przez 15 użytkowników końcowych[38] oraz na podstawie udzielonych wyjaśnień ustalono, że:

- żaden z 15 funkcjonariuszy Komendy objętych badaniem nie prowadził postępowań przygotowawczych z wykorzystaniem systemu e-Posterunek;
- 2 z 15 funkcjonariuszy posiadało nadane hasła i potrafiło zalogować się do e-Posterunku za pomocą indywidualnego hasła, pozostałe 13 osób nie posiadało indywidualnych haseł, nigdy nie używało e-Posterunku oraz nie potrafiło zalogować się do ww. aplikacji (za pomocą hasła dla użytkownika testowego),
- na działających urządzeniach, których użytkownicy byli w stanie zalogować się do aplikacji (2 osoby) zainstalowana była wersja 2.0.8. oraz wersja 1.8.5.0 aplikacji e-Posterunek;
- jeden funkcjonariusz (z WKiPG) potrafił skutecznie wytworzyć podstawowe dokumenty z postępowania przygotowawczego dla fikcyjnego zgłoszenia,
- łącznie w zakładce lista postępowań znajdowały się 2 postępowania (u jednego funkcjonariusza z WKiPG[39]), w zakładce postępowania zakończone nie było żadnego postępowania,
- w wersji 2.0.8. istniała funkcja edycji tworzonych w e-Posterunku dokumentów bezpośrednio przed wydrukiem umożliwiająca modyfikację szaty graficznej,
- 2 urządzenia, których użytkownicy zalogowali się do e-Posterunku nie posiadały mikrofonów, a użytkownicy nie potrafili wskazać funkcji dyktafonu umożliwiającej zapis nagrania na nośniku wskazanym przed uruchomieniem nagrywania;
- wg stanu na dzień 10.01.2013 r. nie działały (na zainstalowanej w Komendzie wersach 1.8.5.0 oraz 2.0.8. aplikacji) funkcjonalności e-Posterunku dotyczące:

[37] Od czasu pierwszej instalacji systemu e-Posterunek, w KMP i jednostkach podległych przeprowadzono około 13.000 postępowań przygotowawczych. Z zastosowaniem systemu e-Posterunek, z powodu nie funkcjonowania systemu, nie przeprowadzono żadnego postępowania przygotowawczego.

[38] Badaniem objęto 15 funkcjonariuszy z Zespołów Dochodzeniowo- Śledczych WKiPG i WK Komendy z 21, którym przekazano sprzęt komputerowy z zainstalowaną aplikacją e-Posterunek. Przeprowadzono oględziny komputerów i aplikacji oraz testy umiejętności użytkowników w zakresie wytworzenia z wykorzystaniem e-Posterunku podstawowych dokumentów postępowania przygotowawczego.

[39] Funkcjonariusz próbował wytworzyć dokumenty w prowadzonym postępowaniu.

możliwości ustanowienia połączenia z SWD; przyjęcia zgłoszenia z e-PUAPu[40] oraz połączenia z KSIP.

(dowód: akta kontroli str. 304-334)

Z udzielonych przez funkcjonariuszy wyjaśnień wynika, iż nie korzystają oni z e-Posterunku, bowiem nigdy nie otrzymali wyraźnego polecenia prowadzenia czynności służbowych przy zastosowaniu tejże aplikacji. Funkcjonariusze wyjaśniali, iż dysponują własną bazą szablonów dokumentów i te narzędzia są im wystarczające do prawidłowego wykonywania czynności służbowych. Ponadto użytkownicy wskazywali, iż nie byli w wystarczający sposób (2 użytkowników) lub w ogóle (13 użytkowników) przeszkoleni z działania e-Posterunku.

(dowód: akta kontroli str. 335-366)

Użytkownik, który jako jedyny potrafił zalogować się do aplikacji wskazał na liczne wady e-Posterunku, w tym brak aktualizacji słowników baz danych (kwalifikacji prawnych), błędne aktualizacje prawne, czasochłonność wprowadzania danych (świadków, pokrzywdzonych) do poszczególnych zakładek, brak możliwości pozostawiania wolnych rubryk w dokumentach, brak funkcji autozapisu (w przypadku braku zasilania tworzone dokumenty zostają bezpowrotnie utracone), funkcjonalność jedynie dla prostych, „jednoczynowych" postępowań (brak ułatwień dla śledztw wielowątkowych), przy próbie połączenia z bazami KSIP uzupełnienie dokumentów nie działa, a program się zawiesza, po czy restartuje (kasując druki wytworzone przed próbą połączenia).

(dowód: akta kontroli str. 349-352)

Otrzymany na potrzeby e-Posterunku sprzęt wykorzystywany był w głównej mierze do generowania dokumentów na potrzeby prowadzonych postępowań, do sporządzania analiz i zestawień oraz do dokonywania sprawdzeń w KSIP.

(dowód: akta kontroli str. 349-352)

Na 6 otrzymanych mobilnych urządzeń dostępowych Twinhead Durabook U12C oraz 3 drukarki mobilne HP Office Jet 100, w KMP użytkowano 2 urządzenia dostępowe i jedną drukarkę[41], zaś 4 urządzenia i 2 drukarki mobilne przekazano do Komisariatów I i II.

(dowód: akta kontroli str. 234-239)

W toku przeprowadzonych oględzin i pobranych wyjaśnień ustalono, że jedno z ww. urządzeń jest użytkowane w terenie przez pracowników WK do sporządzania i edycji dokumentów (bez wykorzystania karty SIM pozwalającej na transmisję danych), zaś drugie z ww. urządzeń mobilnych zostało przekazane do użytkowania funkcjonariuszowi z WKiPG. Drukarka mobilna uległa awarii i została przekazana w dniu 12.12.2012 r. KWP.

(dowód: akta kontroli str. 326, 329, 383)

Przeprowadzone w KMP anonimowe ankiety wśród 20 użytkowników końcowych aplikacji e-Posterunek wykazały m.in.,

- 85% (17 ankietowanych) oceniło, że wprowadzenie aplikacji e-Posterunek nie przyczyniło się do usprawnienia ich pracy i podniesienia jej wydajności, pozostałych 3 nie wyraziło opinii;
- 80% (16) wskazało, że wdrożenie e-Posterunku nie spowodowało zmniejszenia ilości sporządzanej dokumentacji w formie papierowej, 20% (4) nie wyraziło opinii;
- 85% (17) ankietowanych wskazało brak uczestnictwa w szkoleniu z obsługi aplikacji;

[40] Elektroniczna Platforma Usług Administracji Publicznej.
[41] HP OfficeJet 100 nr seryjny MY14P510RH.

- 48% (10) oceniło, że ilość i jakość sprzętu komputerowego w Komendzie nie jest wystarczająca do obsługi e-Posterunku, 24% (5) oceniło, że ilość i jakość sprzętu komputerowego w Komendzie jest wystarczająca, zaś 28% (6) nie miało zdania na ten temat;
- 55% (11) jednoznacznie oceniło e-Posterunek jako zły system, pozostali (45%) nie wyrazili opinii,
- 85% (17) ankietowanych nie korzystało z aplikacji.

W ankietach funkcjonariusze KMP, korzystający z e-Posterunku, wskazywali w szczególności na następujące problemy związane z funkcjonowaniem tej aplikacji: duże wymagania sprzętowe uniemożliwiające prace, brak szkoleń, brak aktualnych druków procesowych, niezbędnych do przeprowadzenia postępowania, brak funkcji edytowania wygenerowanych dokumentów, mała czytelność aplikacji, skomplikowany sposób wprowadzania danych.

(dowód: akta kontroli str. 511-552)

Koordynator ZŁI wyjaśnił, że WRD dysponował 5 zestawami Mobilnych Terminali Przewoźnych[42] zamontowanych w oznakowanych pojazdach. Na ww. sprzęcie nie zainstalowano aplikacji e-Posterunek w celu korzystania z modułu ruchu drogowego. Ponadto wyjaśnił, że poinformował WRD o konieczności dostarczenia ww. pojazdów celem zainstalowania e-Posterunku, jednak *w związku z faktem otrzymywania informacji o wadliwym działaniu aplikacji (błędy merytoryczne i techniczne) zawieszono polecenie instalacji programu e-Posterunek w radiowozach WRD. W sytuacji, kiedy w/w aplikacja nie funkcjonowała w warunkach „produkcyjnych", w czasie służby nie byłoby możliwości testowania modułu Ruchu Drogowego w programie e-Posterunek w radiowozach.* Koordynator ZŁI zadeklarował, że w przypadku uruchomienia ww. aplikacji do fazy produkcyjnej program zostanie niezwłocznie zainstalowany w MTP w ww. pojazdach.

(dowód: akta kontroli str. 562-563)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

Urządzenie mobilne Twinhead Durabook U12C (nr seryjny SY1101000032) przekazane użytkownikowi z WKiPG[43] w dniu 24.01.2012 r., nie było wykorzystywane przez funkcjonariuszy ww. komórki. Przeprowadzone oględziny wykazały, że sprzęt znajdował się w pomieszczeniu użytkownika. Po uruchomieniu systemu został poproszony o „podanie hasła przy pierwszym logowaniu".

(dowód: akta kontroli str. 140, 326)

Z wyjaśnień użytkownika ww. urządzenia mobilnego wynika, iż przyczyną niekorzystania ze sprzętu, był brak możliwości użytkowania wraz z ww. sprzętem posiadanej drukarki stacjonarnej, z powodu braku sterowników drukarki do systemu Windows 7 (zainstalowanym na urządzeniu). Użytkownik nie został wyposażony w drukarkę przenośną.

(dowód: akta kontroli str. 357-358)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonej nieprawidłowości, działalność KMP w badanym obszarze.

[42] Dalej „MTP"

[43] Naczelnik WKiPG odebrał ww. sprzęt w dniu 24.01.2012 r. – sprzęt przechowywany był w gabinecie użytkownika Andrzeja Lorka, któremu poleceniem ustnym przydzielono ww. sprzęt.

3. Zabezpieczenie danych osobowych przetwarzanych w aplikacjach SWD i e-Posterunek.

3.1. SWD

Opis stanu faktycznego

KMP otrzymała opracowane na szczeblu Komendy Głównej Policji dokumenty, o których mowa w § 3 rozporządzenia MSWiA z dnia 29 kwietnia 2004 r., tj.: „Politykę bezpieczeństwa systemu wspomagania dowodzenia jednostek organizacyjnych Policji – poziom wysoki”[44], oraz „Instrukcję zarządzania systemem teleinformatycznym przetwarzającym dane osobowe – system wspomagania dowodzenia jednostek organizacyjnych Policji – poziom wysoki”[45], dotyczące zabezpieczenia danych osobowych przetwarzanych w SWD.

(dowód: akta kontroli str. 18-53)

Decyzją z 13.03.2012 r. Komendant KMP, zgodnie z wymogami decyzji Komendanta Wojewódzkiego z dnia 21.11.2011 r., wyznaczył lokalnych administratorów SWD w KMP, co zostało opisane w punkcie 1.1. wystąpienia.

(dowód: akta kontroli str. 68)

Zapoznanie z dokumentami dotyczącymi ochrony danych osobowych przetwarzanych w systemie, w tym z polityką bezpieczeństwa SWD oraz instrukcją zarządzania SWD potwierdziło pisemnie 85 użytkowników SWD z KMP, Komisariatu I i Komisariatu II.

(dowód: akta kontroli str. 368-373)

Oględziny 4 komputerów do obsługi SWD (2 w WRD i 2 w WP) wykazały, że przy korzystaniu z systemu stosuje się uwierzytelnianie uprawnionego użytkownika zgodnie z wymogami określonymi w ww. instrukcji zarządzania SWD, poprzez uwierzytelnienie i autoryzację za pomocą karty mikroprocesorowej oraz kodu PIN jednoznacznie przypisanego użytkownikowi.

(dowód: akta kontroli str. 248-295)

Logowanie do systemu Windows na 2 komputerach odbywało się za pomocą karty mikroprocesorowej oraz kodu PIN (stanowisko dyżurnych z WP i odprawiających z WRD), a na 2 pozostałych wg zasad określonych w systemie Windows za pomocą identyfikatora oraz minimum 8-znakowego hasła, o ważności maksymalnie 90 dni (komputer Naczelnika WRD i zastępcy Naczelnika WP). Objęte oględzinami komputery posiadały zainstalowany program szyfrujący TrueCrypt, umożliwiający stosowanie kryptograficznych metod ochrony danych. Zabezpieczenie przed działaniem szkodliwego oprogramowania zrealizowano za pomocą programu antywirusowego Dr.Web for Windows z uaktualnioną bazą wirusów na dzień 4.01.2013 r. Komputery wykorzystywane do obsługi aplikacji SWD nie miały połączenia z Internetem, połączone były jedynie z wewnętrzną siecią PSTD[46]. Stosownie do wymogów określonych dla stanowisk dostępowych sieci PSTD[47] dostęp do BIOS-u 3 badanych komputerów był zabezpieczony hasłem. W jednym przypadku (komputer Naczelnika WP) hasło na BIOS zostało założone przez administratora w toku dokonywanych oględzin. Użytkownicy systemu badanych komputerów korzystali z kont z ograniczonymi uprawnieniami (grupa Użytkownicy).

(dowód: akta kontroli str. 248-295, 374-382)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

[44] Zwanej dalej „polityką bezpieczeństwa SWD”.
[45] Zwanej dalej „instrukcją zarządzania SWD”.
[46] Policyjna Sieć Transmisji Danych
[47] Zalecenia dotyczące standardów technicznych , użytkowych oraz bezpieczeństwa, stosowanych w Policji, w zakresie informatyki i łączności z 29.03.2012 r.

W przypadku 2 urządzeń do obsługi SWD[48] zastosowano maksymalny termin zmiany hasła do systemu operacyjnego Windows dłuższy niż 30 dni[49], co nie spełniało wymogów określonych w pkt IV ppkt 2 załącznika do ww. rozporządzenia Ministra Spraw Wewnętrznych i Administracji.

(dowód: akta kontroli str. 374-382)

Koordynator Zespołu Łączności i Informatyki KMP[50] wyjaśnił, że definiowanie długości haseł do systemu operacyjnego zostało oparte na zapisach zaleceń ws. standardów bezpieczeństwa, zatwierdzonych przez zastępcę Komendanta Głównego Policji.

(dowód: akta kontroli str. 431-432)

Uwagi dotyczące badanej działalności

Żaden z badanych komputerów nie był podłączony do elektrycznej sieci zasilającej za pośrednictwem zasilacza awaryjnego (np. UPS), lecz tylko do wydzielonej sieci zabezpieczonej bezpiecznikami różnicowymi, w celu zapobieżenia ewentualnej utraty danych spowodowanej zakłóceniami w sieci zasilającej.

(dowód: akta kontroli str. 374-382)

Koordynator ZŁI wyjaśnił, że zgodnie *z polityką bezpieczeństwa systemu SWD w p. 3 ppkt. 8 wymagania bezpieczeństwa danych osobowych są realizowane poprzez zapewnienie: m.in.: „podłączenie komputerów, w których przetwarzane są dane osobowe do lokalnej sieci zasilającej lub UPS". Jak wynika z powyższego w KMP w Koszalinie wymagania bezpieczeństwa w zakresie m.in. bezpieczeństwa danych osobowych są zapewnione.*

(dowód: akta kontroli str. 384-386)

Ocena cząstkowa

Najwyższa Izba Kontroli pozytywnie ocenia działalność KMP w zbadanym zakresie.

3.2. E-Posterunek

Opis stanu faktycznego

W KMP nie opracowano żadnych procedur zabezpieczenia danych osobowych przetwarzanych w e-Posterunku. Decyzją z dnia 23.02.2012 r. Komendant KMP wyznaczył administratora systemu teleinformatycznego w KMP (Koordynator ZŁI) oraz inspektora bezpieczeństwa teleinformatycznego w KMP, będącego jednocześnie administratorem lokalnym e-Posterunku.

(dowód: akta kontroli str. 7-8, 387)

Komendant wyjaśnił, że KMP nie otrzymała odgórnego aktu prawnego regulującego funkcjonowanie systemu e-Posterunek w postaci zarządzenia, instrukcji zarządzania tymże systemem informatycznym przetwarzającym dane osobowe, zatwierdzonej przez Komendanta Głównego Policji, dokumentu stanowiącego podstawę do tego, aby można było przetwarzać w tym systemie właściwe dane osobowe. Z założenia uznano zatem, iż aplikacja ta jest aplikacją testową i nie przeprowadzono do dnia dzisiejszego, żadnego postępowania.

(dowód: akta kontroli str. 79-82)

W KMP otrzymał do stosowania „Wytyczne Dyrektora Biura Łączności i Informatyki KGP w sprawie standardów technicznych, użytkowych oraz bezpieczeństwa, stosowanych w Policji w zakresie informatyki i łączności" z 6.07.2010 r. oraz „Zalecenia dotyczących standardów technicznych, użytkowych oraz

[48] Zestawy komputerowe Topadvert 1100S użytkowany przez Zastępca Naczelnika WP oraz Fujitsu-Siemens Scenic użytkowany przez Naczelnika WRD

[49] Tj. 90 dni.

[50] Dalej *Koordynator ZŁI*.

bezpieczeństwa, stosowanych w policji w zakresie informatyki i łączności" z 29.03.2012 r.[51]

(dowód: akta kontroli str. 388-430)

Oględziny 15 stacji dostępowych przeznaczonych do obsługi aplikacji e-Posterunek, w tym 7 komputerów stacjonarnych i 8 komputerów przenośnych (6 notebooków i 2 dostępowych urządzeń mobilnych) wykazały, iż każdy użytkownik posiadał w systemie Windows swoje indywidualne konto z ograniczonymi uprawnieniami. Instalacja dodatkowego oprogramowania możliwa była jedynie z poziomu administratora. Urządzenia nie były podłączone do sieci zewnętrznej, a jedynie do sieci PSTD. Dostęp do systemu Windows był zabezpieczony hasłami dostępowymi składającymi się z minimum 8 znaków zawierającymi cyfry oraz znaki specjalne (12 komputerów) lub dostęp za pośrednictwem systemu eGina, wymagającego użycia karty mikroprocesorowej i indywidualnego numeru PIN. Ponadto na każdym z komputerów dostęp do BIOS był zabezpieczonych hasłem. Dostępowe urządzenia mobilne oraz notebooki miały zainstalowane i uruchomione aplikacje szyfrujące TrueCrypt umożliwiające stosowanie kryptograficznych metod ochrony danych. Na 11 (z 15) urządzeniach zainstalowane było aktualne oprogramowanie antywirusowe.

(dowód: akta kontroli str. 374-382)

Spośród 15 użytkowników komputerów, 13 nie potrafiło zalogować się do systemu e-Posterunek, a 2 użytkowników zalogowało się do ww. aplikacji za pomocą 6-cyfrowego loginu oraz indywidualnych haseł dostępu.

(dowód: akta kontroli str. 304-334)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

KMP nie zastosowała następujących zabezpieczeń technicznych wymaganych na podstawie art. 36 ust. 1 ustawy o ochronie danych osobowych, załącznika do rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, a także wewnętrznych regulacji Komendy przyjętych w tym zakresie:

1. W przypadku 2 użytkowników, którzy potrafili zalogować się do e-Posterunku, aplikacja nie wymuszała regularnej zmiany haseł dostępowych, ani nie wymuszała na użytkowniku zastosowania w haśle minimum 8 znaków, co nie spełniało wymogów określonych w pkt IV ppkt 2 oraz pkt VIII załącznika do ww. rozporządzenia Ministra Spraw Wewnętrznych i Administracji oraz zaleceń ws. standardów bezpieczeństwa. Użytkownicy nie zmienili swojego hasła od daty pierwszego logowania do danej wersji aplikacji tj. odpowiednio od lipca 2011 r. i listopada 2012 r. oraz stosowali hasła dostępu, które składały się z mniejszej niż 8 liczby znaków (tj. odpowiednio 5 i 6 znaków).

(dowód: akta kontroli str. 304-321)

Zgodnie z p. IV ppkt 2 załącznika do ww. rozporządzenia Ministra Spraw Wewnętrznych i Administracji w przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni, a zgodnie z pkt VIII ww. załącznika oraz zaleceniami ws. standardów bezpieczeństwa (w rozdziale 8 pkt 7 lit. b-e) hasła powinny mieć długość minimum 8 znaków.

(dowód: akta kontroli str. 424)

[51] Zwanych dalej „zaleceniami ws. standardów bezpieczeństwa".

Koordynator ZŁI w sprawie haseł do e-Posterunku wyjaśnił, że definiowanie długości haseł *określone jest na poziomie projektowania systemu przez producenta i nie jest możliwe na poziomie konta administratora. W związku z powyższym administrator w KMP nie ma możliwości zdefiniowania parametrów haseł wymuszanych przez system e-Posterunek a są one narzucone przez program.*

(dowód: akta kontroli str. 384-386)

2. W przypadku 11 urządzeń zastosowano maksymalny termin zmiany hasła do systemu operacyjnego dłuższy niż 30 dni, co nie spełniało wymogów określonych w pkt IV ppkt 2 załącznika do ww. rozporządzenia Ministra Spraw Wewnętrznych i Administracji. Maksymalny termin zmiany hasła do systemu Windows wynosił 90 dni dla 11 urządzeń do obsługi e-Posterunku (3 urządzenia użytkowane w WKiPG[52], 6 w WK[53] oraz 1 w WP[54]).

(dowód: akta kontroli str. 374-382)

Koordynator ZŁI wyjaśnił, że definiowanie długości haseł do systemu operacyjnego zostało oparte na zapisach zaleceń ws. standardów bezpieczeństwa, zatwierdzonych przez zastępcę Komendanta Głównego Policji.

(dowód: akta kontroli str. 431-432)

3. W przypadku 4 z 15 sprawdzanych komputerów nie zapewniono właściwej ochrony antywirusowej przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, w szczególności przed wirusami, trojanami i robakami internetowymi, co było niezgodne z pkt III ppkt 1 załącznika do ww. rozporządzenia Ministra Spraw Wewnętrznych i Administracji oraz zaleceniami ws. standardów bezpieczeństwa. Na dostępowym urządzeniu mobilnym[55], wykorzystywanym przez pracownika Zespołu Dochodzeniowo - Śledczego WKiPG nie zainstalowano programu antywirusowego, zaś na dostępowym urządzeniu mobilnym[56], wykorzystywanym przez pracownika Zespołu Dochodzeniowo - Śledczego WK, pomimo zainstalowania oprogramowania Dr.Web 6.00.4 było ono nieaktywne bez aktualnych baz danych o zabezpieczeniach (systemowy komunikat: „Antywirusowe bazy danych są nieaktualne."). Na 2 komputerach (notebook[57], komputer stacjonarny[58]) użytkowanych przez pracowników Zespołu Dochodzeniowo - Śledczego WK zainstalowano takie oprogramowanie lecz nie aktualizowano baz wirusów (bazy wirusów odpowiednio z 13.01.2012 r. oraz 7.11.2011 r.)

(dowód: akta kontroli str. 374-382)

Zgodnie z p. III ppkt 1 załącznika do ww. rozporządzenia Ministra Spraw Wewnętrznych i Administracji system informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

Koordynator ZŁI w sprawie zapewnienia aktualnego oprogramowania antywirusowego wyjaśnił, że *dodatkowe nie wbudowane w system Windows programy antywirusowe aktualizowane są poprzez sieć PSTD z serwera wewnętrznego. W przypadku odłączenia sprzętu komputerowego od sieci PSTD nie nastąpi aktualizacja baz wirusów, co nie znaczy, że program nie funkcjonuje.*

---

[52] Urządzenie mobilne Twinhead Durabook U12C o nr ser. SY1101000032 i 2 Notebooki Lenovo o nr seryjnych LR1EW7R, LR1EX0R.

[53] 4 Notebooki Lenovo o nr ser. LR1EW8L, LR1EW4T, LR1EW5N, LR1EX3A, komputer stacjonarny Topadvert 1100S o nr ser. S24JJ9GB601385, urządzenie mobilne Twinhead Durabook U12C o nr ser. SY1101000995.

[54] Komputer stacjonarny Topadvert 1100S o nr ser. WP S24JJ90B626668.

[55] Nr seryjny SY1101000032.

[56] Nr seryjny SY1101000995.

[57] Pokój nr 325 WK KMP – nr seryjny LR1EW4T.

[58] Pokój nr 313 WK KMP – Topadvert 1100S nr seryjny S24JJ9GB601385.

W jednym z komputerów, w którym nie było zainstalowanego oprogramowania antywirusowego zaistniał problem techniczny z dodatkową aplikacją antywirusów i wykorzystano systemowe oprogramowanie zabezpieczające Windows, aktualnie problem jest na etapie rozwiązania.

(dowód: akta kontroli str.384-386)

Uwagi dotyczące badanej działalności

Żaden z 7 zestawów komputerów stacjonarnych nie był podłączony do elektrycznej sieci zasilającej za pośrednictwem zasilacza awaryjnego UPS. Ww. sprzęt był podłączony do wydzielonej sieci zabezpieczonej bezpiecznikami różnicowymi, w celu zapobieżenia ewentualnej utraty danych.

(dowód: akta kontroli str. 374-382)

Koordynator ZŁI wyjaśnił, że *zgodnie z wymaganiami i zaleceniami bezpieczeństwa* w KMP *z wyjątkiem części priorytetowego sprzętu komputerowego który podłączony jest do sieci z napięciem dedykowanym (z podtrzymaniem napięcia w przypadku jego zaników) wszystkie komputery w Komendzie i jednostkach podległych podłączone są do elektrycznej sieci wydzielonej przeznaczonej dla sprzętu komputerowego*.

(dowód: akta kontroli str. 384-386)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, działalność KMP w badanym obszarze.

IV. Wnioski.

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[59], wnosi o:

1. Uruchomienie SWD na stanowiskach pracy funkcjonariuszy dowodzących w WK i WKiPG.
2. Podjęcie działań organizacyjnych, zmierzających do objęcia szkoleniem wszystkich pracowników służb dochodzeniowo-śledczych, których przewidziano do obsługi e-Posterunku.
3. Bieżące aktualizowanie wersji e-Posterunku zainstalowanych na urządzeniach.
4. Podjęcie działań zmierzających do wykorzystania otrzymanych dostępowych urządzeń mobilnych Twinhead Durabook U12C, zgodnie z ich przeznaczeniem.
5. Podjęcie działań w celu zapewnienia prawidłowego zabezpieczenia sprzętu informatycznego obsługującego w KWP aplikację SWD i e-Posterunek przed nieuprawnionym dostępem, w tym dokonanie przeglądu urządzeń nieobjętych kontrolą NIK.

[59] Dz. U. z 2012 r., poz. 82.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ust. 1 i 2 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do Dyrektora Delegatury NIK w Szczecinie.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 14 dni od dnia otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i wykonania wniosków oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Szczecin, dnia stycznia 2013 r.

Najwyższa Izba Kontroli
Delegatura w Szczecinie

Kontroler
Maciej Mikulski
specjalista kontroli państwowej

.....
Podpis

.....
Podpis

Kontroler
Krzysztof Szczepaniak
specjalista kontroli państwowej

.....
Podpis