NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie

LSZ – 4101-26-01/2012
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

1. Jarosław Staniszewski, doradca ekonomiczny, upoważnienie do kontroli nr 83614 z dnia 16.10.2012 r.

(dowód: akta kontroli str. 1)

2. Tomasz Cyranka, gł. specjalista k.p., upoważnienie do kontroli nr 85159 z dnia 21.11.2012 r.

(dowód: akta kontroli str. 3)

Jednostka kontrolowana

Komenda Powiatowa Policji w Policach[1], ul. Kasprowicza 3, 72-010 Police.

Kierownik jednostki kontrolowanej

Andrzej Zakrzewski, podinspektor, Komendant Komendy Powiatowej Policji w Policach[2].

(dowód: akta kontroli str. 5)

II. Ocena kontrolowanej działalności

1. System Wspomagania Dowodzenia[3].

Ocena ogólna

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości[4], wdrożenie i funkcjonowanie w KPP systemu SWD.

Uzasadnienie oceny ogólnej

SWD był podstawowym narzędziem pracy służby dyżurnej w KPP. W systemie były rejestrowane wszystkie wymagające tego zgłoszenia, zdarzenia oraz czynności związane z reakcją Policji. Na bieżąco wprowadzano dyslokację służb patrolowo-interwencyjnych oraz zespołów dochodzeniowo-śledczych. Stwierdzono, że urządzenia i sprzęt komputerowy otrzymane do obsługi SWD były wykorzystywane w sposób zgodny z przeznaczeniem.

Stwierdzone nieprawidłowości dotyczyły:
- nieprzestrzegania procedur dotyczących udzielania upoważnień dostępu do SWD określonych w „Polityce bezpieczeństwa Systemu Wspomagania Dowodzenia jednostek organizacyjnych Policji - poziom wysoki”[5],
- niezabezpieczenia części sprzętu informatycznego obsługującego SWD przed nieuprawnionym dostępem.

---

[1] Dalej: *KPP*.
[2] Dalej: *Komendant*.
[3] Dalej: *SWD*.
[4] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.
[5] Opracowaną w 2012 r. przez Biuro Łączności i Informatyki KGP przy współpracy Głównego Sztabu Policji KGP oraz Biura Ochrony Informacji Niejawnych KGP, zatwierdzoną przez Komendanta Głównego Policji, zwana dalej: *Polityką bezpieczeństwa SWD*.

2. E-Posterunek.

Ocena ogólna

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

Uzasadnienie oceny ogólnej

Aplikacja e-Posterunek była wykorzystywana w Komendzie w niewielkim zakresie. Komendant nie miał decydującego wpływu na określenie terminu wprowadzenia do użytkowania tej aplikacji, ani na zapewnienie warunków technicznych jej funkcjonowania. W powyższym zakresie KPP nie otrzymała wytycznych od jednostek organizacyjnych wyższego szczebla, tj. od Komendy Wojewódzkiej Policji[6] i Komendy Głównej Policji[7].

Stwierdzone nieprawidłowości dotyczyły w szczególności:
- prowadzenia w aplikacji e-Posterunek postępowań przygotowawczych, mimo nieopracowania do dnia zakończenia kontroli NIK dla e-Posterunku, wymaganych na podstawie art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[8] oraz § 3 rozporządzenia MSWiA z dnia 29 kwietnia 2004 r.[9], dokumentacji, tj.: Polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
- niezabezpieczenia części sprzętu informatycznego obsługującego aplikację e-Posterunek przed nieuprawnionym dostępem.

III. Opis ustalonego stanu faktycznego

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

1.1. SWD

Opis stanu faktycznego

Komendant Wojewódzki Policji w Szczecinie[10] decyzją z 21.11.2011 r.[11] w sprawie wprowadzenia do użytku w jednostkach organizacyjnych Policji województwa zachodniopomorskiego SWD, postanowił wdrożyć system w terminach: KWP i KMP w Szczecinie – 21 listopada 2011 r., KMP w Koszalinie – do 5 grudnia 2011 r., a w pozostałych jednostkach – nie później niż do 31 grudnia 2012 r. W dniu 14.05.2012 r. wpłynęło do KPP pismo Pierwszego Zastępcy Komendanta Głównego Policji informujące m.in. o zmianach dotyczących wewnętrznych przepisów prawnych, umożliwiających wykonywanie w jednostkach organizacyjnych Policji czynności polegających na obsłudze zgłoszeń z numeru alarmowego 112 przez operatorów zatrudnionych w urzędach wojewódzkich.

(dowód: akta kontroli str. 37, 39, 549, 554-558)

W KPP poza opracowaniem charakterystyki obszaru przetwarzania danych osobowych w SWD[12], nie opracowano żadnych wewnętrznych aktów prawnych lub procedur dotyczących zasad organizacji pracy komórek organizacyjnych z wykorzystaniem SWD. Wdrożenie systemu odbywało się m.in. poprzez

---

[6] Dalej: *KWP*.
[7] Dalej: *KGP*.
[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] Dalej: Komendant Wojewódzki.
[11] Nr 318/11.
[12] W której określono jednostkę organizacyjną, nazwę i numer pomieszczenia oraz część budynku i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe w komórkach organizacyjnych KPP.

wyznaczenie na polecenie Komendanta Wojewódzkiego[13]: Lokalnego administratora merytorycznego SWD[14], Lokalnego administratora technicznego SWD[15] i Lokalnego administratora bezpieczeństwa Informacji[16].

(dowód: akta kontroli str. 37, 39, 42, 43, 549, 551-553, 582, 583)

Komendant wyjaśnił, że w przypadku SWD *brak było polecenia jednostki wyższego rzędu, aby wydawać wewnętrzne akty prawne. Wdrożenie systemu odbywało się m.in. poprzez wyznaczenie użytkowników systemu przez (…) lokalnego administratora SWD, biorąc pod uwagę sprawowaną funkcję, potrzeby służby i realizowane zadania, a także opracowanie charakterystyki obszaru przetwarzania danych osobowych; sprawdzenie sprzętu przez lokalnego administratora technicznego SWD, a także wgrywanie i konfigurowanie programu, monitorowanie błędów, sporządzenie map, sektorów dla Ogniwa Patrolowo-Interwencyjnego, rejonów dzielnicowych*.

(dowód: akta kontroli str. 37, 39)

KPP otrzymała 19.11.2008 r. 3 zestawy komputerowe do obsługi SWD[17], z których 2 zainstalowano na stanowiskach dyżurnych oraz 1 w pokoju Zastępcy Naczelnika Wydziału Kryminalnego[18] KPP. Ponadto SWD został zainstalowany na 9 zestawach komputerowych (otrzymanych w latach 2005-2009), które przed instalacją systemu wykorzystywane były w KPP głównie do sprawdzania danych w Krajowym Systemie Informacyjnym Policji[19]. Pierwsza instalacja oprogramowania SWD w KPP została przeprowadzona samodzielnie w okresie 10-14.09.2012 r. przez administratora technicznego SWD. Urządzenia wykorzystywane były jako stanowiska dostępowe do KSIP i innych baz danych oraz do dnia 18.09.2012 r. (uruchomienia SWD w KPP) - do obsługi Elektronicznej Książki Służby Dyżurnego[20].

(dowód: akta kontroli str. 23, 28-29, 30-36, 106-151, 549)

W okresie objętym kontrolą KPP, na wniosek KWP, dokonała 1 analizy potrzeb sprzętowych do wdrożenia w jednostce SWD. KPP w odpowiedzi na pismo z 30.04.2012 r.[21], wnioskowała o 9 stacji dostępowych (potrzeby obejmowały również Komisariat Policji w Mierzynie[22]).

(dowód: akta kontroli str. 545-548)

Administrator systemów teleinformatycznych wyjaśnił, że do dnia 11.01.2013 r. nie otrzymano żadnej informacji w ww. sprawie. Ponadto wyjaśnił, że *w sprawie doposażenia stanowisk pracujących z aplikacją SWD kilkakrotnie zwracano się telefonicznie z prośbą do pracowników KWP o zakup dodatkowych kart pamięci RAM typu DDR 1. W związku z nieotrzymywaniem odpowiedzi na telefoniczne zamówienia dnia 05.11.2012 r. wysłano elektroniczną policyjną pocztą LOTUS zapotrzebowanie na w/w elementy*. Pamięć RAM (6 szt.) KPP otrzymała w dniu 11.12.2012 r.

(dowód: akta kontroli str. 542, 543)

W KPP był wykorzystywany system raportowania o usterkach w funkcjonowaniu oprogramowania SWD, który został opracowany w pierwszym kwartale 2012 r.

---

13 Pismo z 12.12.2011 r. nr WS-0400-1790/11.
14 Naczelnik Wydziału PiRD KPP.
15 Starszy technik w Zespole Łączności i Informatyki KPP.
16 Starszy inspektor w Zespole Ochrony Informacji Niejawnych oraz w Zespole Łączności i Informatyki KPP.
17 3 zestawy komputerowe (procesor 2,5 Ghz, pamięć RAM 2 GB, dysk twardy 250 GB), 4 monitory LCD 19" Asus VB 191T (niepanoramiczne), telewizor LCD 32", czytniki kart mikroprocesorowych (3), 2 drukarki laserowe mono oraz drukarka laserowa sieciowa kolorowa.
18 Dalej: *WK*.
19 Dalej: *KSIP*.
20 Dalej: *EKSD*.
21 ŁI-0151-760/12.
22 Dalej: *KP Mierzyn*.

przez KGP[23]. Zgodnie z jego treścią komunikaty dotyczące zgłaszanych nieprawidłowości w funkcjonowaniu SWD mogły być kierowane przez użytkowników do Biura Łączności i Informatyki KGP; zamieszczane poprzez forum użytkowników w Policyjnej Platformie Wdrożeniowej[24] oraz na liście dyskusyjnej „startswd" na platformie Internetu. Na forum PPW miały być zamieszczane wszystkie zgłoszenia przekazane przez użytkowników i zakwalifikowane jako błędy działania systemu wraz z informacją o stanie ich realizacji.

(dowód: akta kontroli str. 549)

Komendant w sprawie konsultowania się jednostek wyższego stopnia na etapie określania założeń SWD oraz w okresie tworzenia ww. systemu, wyjaśnił, że *nie zwracano się o opinie dotyczące praktycznych aspektów*.

(dowód: akta kontroli str. 37, 40)

Według stanu na 10.12.2012 r. aplikacja SWD została zainstalowana na 18 stacjach dostępowych, z tego: 9 w Wydziale Prewencji i Ruchu Drogowego KPP[25] (w tym 2 w Zespole Dyżurnych), 2 w WK, 1 w Zespole Łączności i Informatyki oraz 6 w KP w Mierzynie.

(dowód: akta kontroli str. 30, 31-36, 109, 117-119)

Na dzień 21.10.2012 r. upoważnienia do obsługi systemu SWD otrzymało 30 osób[26], w zależności od zakresu uprawnień i wykonywanych obowiązków służbowych.

(dowód: akta kontroli str. 44-46)

Spośród 30 użytkowników SWD:

- 20 zostało przeszkolonych przez funkcjonariuszy KWP - szkolenia odbywały się w kilku jednodniowych terminach, w okresie od 13.02.2012 r. do 13.03.2012 r. w wymiarze 7 godzin, obejmujących praktyczną obsługę systemu,
- 14 uczestniczyło w 5 godzinnej multimedialnej prezentacji obsługi programu SWD prowadzonej 12.09.2012 r. przez funkcjonariusza KGP, obejmującej pokaz praktycznej obsługi systemu,
- 13 uczestniczyło 12.09.2012 r. w szkoleniu teoretycznym (1 godzina) z zakresu ochrony danych osobowych podczas przetwarzania danych w SWD oraz polityki bezpieczeństwa SWD,
- 12 funkcjonariuszy KPP i KP w Mierzynie uczestniczyło 17.09.2012 r. w szkoleniu obejmującym praktyczną obsługę systemu (6 godzin),
- 3 funkcjonariuszy KP w Mierzynie, którzy nie zostali przeszkoleni z obsługi systemu SWD w ww. terminach, po wprowadzeniu SWD odbyli indywidualny instruktaż prowadzony przez Kierownika Referatu Prewencji KP w Mierzynie.

(dowód: akta kontroli str. 47-49, 50-61)

Komendant w sprawie osiągnięcia docelowego stanu sprzętu, instalacji systemu SWD, przeszkolenia i upoważnienia użytkowników, wyjaśnił, że *planowane jest rozszerzanie ilości użytkowników, ale dopiero w przypadku otrzymania niezbędnej ilości sprzętu. Sam sprzęt w systemie SWD nie spełnia wymogów (parametrów – spełniają tylko 3) do pełnego wykorzystania min. poprzez złe parametry monitorów (powinny być panoramiczne), zbyt małą pamięć operacyjną*.

(dowód: akta kontroli str. 37, 40)

Ustalone nieprawidłowości

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

[23] Pismo Zastępcy Komendanta Głównego Policji z 28.03.2012 r.
[24] Dalej: *PPW*.
[25] Dalej: Wydział PiRD.
[26] 28 funkcjonariuszy/pracowników KPP Police oraz Komisariatu w Mierzynie oraz 2 pracowników Zespołu Łączności i Informatyki KPP.

Spośród 30 użytkowników którzy otrzymali upoważnienia do pracy w SWD:

- 1 użytkownik, który upoważnienie otrzymał 17.09.2012 r., odbył 16.02.2012 r. szkolenie w KWP obejmujące praktyczną obsługę systemu, natomiast nie został zapoznany i nie podpisał oświadczenia (wg wzoru stanowiącego załącznik nr 2 do polityki bezpieczeństwa SWD) o zapoznaniu się z przepisami ustawy o ochronie danych osobowych oraz wewnętrznymi aktami prawnymi i dokumentami dotyczącymi ochrony danych osobowych, w tym z polityką bezpieczeństwa SWD oraz „Instrukcją zarządzania systemem teleinformatycznym przetwarzającym dane osobowe - SWD jednostek organizacyjnych Policji - poziom wysoki"[27],
- 3 funkcjonariuszom/pracownikom upoważnienia zostały wydane odpowiednio na: 13 dni (2 pracownikom) i na 9 dni (1 funkcjonariuszowi) przed zapoznaniem i podpisaniem ww. oświadczenia.

(dowód: akta kontroli str. 44-45, 60-61)

Według pkt. 1.7 Polityki bezpieczeństwa SWD, wszystkie osoby przed uzyskaniem upoważnienia muszą zostać przeszkolone w zakresie wykonywania czynności zapewniających ochronę danych osobowych oraz zapoznane z dokumentacją bezpieczeństwa. W pkt 3 m.in. stwierdzono, że wymagania bezpieczeństwa danych osobowych są realizowane poprzez zapewnienie przetwarzania danych osobowych w systemie SDW tylko przez osoby przeszkolone i upoważnione. W pkt 8 *Szkolenia* m.in. zapisano, że dla zapewnienia odpowiedniego poziomu bezpieczeństwa systemu informatycznego SWD dla wszystkich użytkowników, w jednostkach organizacyjnych Policji prowadzone są obowiązkowe szkolenia w zakresie obsługi aplikacji SWD.

(dowód: akta kontroli str. 590, 593, 599)

Naczelnik Wydziału PiRD wyjaśnił, że funkcjonariusz *nie został zapoznany z aktami prawnymi dotyczącymi funkcjonowania SWD, gdyż po odbytym już szkoleniu w KWP zmienił stanowisko pracy, gdzie nie jest wymagane SWD*. Ponadto wyjaśnił, że *różnice w dniach zapoznania z dniami nadania uprawnień nie były znaczne. Funkcjonariusze rozpoczęli pracę w systemie SWD dopiero po zatwierdzeniu i otrzymaniu uprawnień*.

(dowód: akta kontroli str. 73-75, 540-541)

Uwagi dotyczące badanej działalności

Spośród 30 użytkowników którzy otrzymali upoważnienia do pracy w SWD, 3 nie zostało zapoznanych z zarządzeniem 453/11 Komendanta Głównego Policji z dnia 27.04.2011 r. w sprawie form i metod przetwarzania informacji wspomagających kierowanie niektórymi działaniami Policji podejmowanymi w celu wykonywania zadań ustawowych.

(dowód: akta kontroli str. 51)

Naczelnik Wydziału PiRD wyjaśnił: niezapoznanie 3 funkcjonariuszy z zarządzeniem (…) wiąże się ze zwykłym niedopatrzeniem. (…) *podjęto czynności zmierzające do zapoznania policjantów i pracowników z w/w Zarządzeniem.* (…) *Zarządzenie (…) jest aktem prawa ogólnodostępnym i każda z osób bez problemu mogła uzyskać akt i zapoznać się z nim. Osoby, których nie zapoznano pełniły raczej role techniczne przy wprowadzaniu SWD (informatycy, pracownicy cywilni). W pierwszej kolejności skupiłem się na zapoznaniu z wszystkimi dokumentami i aktami prawnymi osoby na co dzień użytkujące i wyznaczone do pracy przy systemie SWD*.

(dowód: akta kontroli str. 540-541)

[27] Opracowaną w 2012 r. przez Biuro Łączności i Informatyki KGP przy współpracy Głównego Sztabu Policji KGP oraz Biura Ochrony Informacji Niejawnych KGP, zatwierdzoną przez Komendanta Głównego Policji, zwana dalej: *Instrukcją zarządzania SWD*.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości działalność kontrolowanej jednostki w zbadanym zakresie.

1.2. E-Posterunek

Opis stanu faktycznego

W związku z otrzymanym Harmonogramem prac wdrożeniowych określonych w piśmie Zastępcy Komendanta Głównego Policji z 8 czerwca 2010 r. (nr Lj. 73/10) zakładającym m.in. wdrożenie aplikacji e-Posterunek w KWP do końca października 2010 r. oraz pismem Dyrektora Biura Kryminalnego KGP z 6 września 2010 r. (nr Ads-745/10) informującym o udostępnieniu wersji instalacyjnej aplikacji e-Posterunek i umieszczeniu jej w Centrum Dystrybucji Oprogramowania[28] do pobrania i wdrożenia, z-ca Komendanta Wojewódzkiego Policji pismem z 13 września 2010 r. (nr DA-I-0402-60/10/AB) poinformował Komendantów Miejskich/Powiatowych Policji o umieszczeniu w CDO wersji instalacyjnej aplikacji e-Posterunek oraz dokumentacji pomocniczej (Podręcznik użytkowania i Podręcznik administratora). W pismach z 11.01.2012 r. oraz 30.04.2012 r. (nr Li 898/12) KWP informowała m.in. o: udostępnieniu wersji 2.0 aplikacji e-Posterunek, rozbudowaniu aplikacji o moduł ruchu drogowego i możliwość współpracy tego modułu z KSIP.

(dowód: akta kontroli str. 549-550, 563-565, 577-580)

W KPP nie opracowano żadnych wewnętrznych aktów prawnych ani procedur dotyczących zasad organizacji pracy komórek organizacyjnych Komendy z wykorzystaniem systemu e-Posterunek.

(dowód: akta kontroli str. 549)

Komendant w sprawie działań organizacyjnych podjętych w celu wdrożenia systemu e-Posterunek wyjaśnił, że *nie ma żadnej decyzji o wprowadzeniu aplikacji, ale z poleceń służbowych zawieranych w pismach wynika, że po otrzymaniu sprzętu oraz przeszkoleniu policjantów system e-Posterunek ma być wdrożony. Świadczą o tym min. pisma dot. monitorowania błędów tj. DA-I-0402-60/10/AB z KWP z dnia 15.02.2011 r. oraz pismo l.dz j.w z dnia 18.02.2011 r., w którym należało złożyć informację na temat funkcjonowania e-Posterunku. Nadto pismem nr DA-I-0402-53/12/RL z KWP z 09.05.2012 r. należało udzielić informacji o ilości funkcjonariuszy wykorzystujących aplikację, ilość prowadzonych z jej wykorzystaniem postępowań oraz uwag i spostrzeżeń do wersji e-Posterunek 2*. Ponadto wyjaśnił, że w ramach wdrożenia systemu e-Posterunek, *zgodnie z pismem nr DA-I-0402-60/10/AB z dnia 13.09.2010 r. z KWP, wytypowano do przeszkolenia funkcjonariusza, który po odbytym szkoleniu, szkolił z zakresu aplikacji e-Posterunek pozostałych policjantów realizujących zadania dochodzeniowo-śledcze. Szkolenie wytypowanego funkcjonariusza przeprowadzono w dniu 21.09.2010 r., a następnie szkolenie funkcjonariuszy KPP w Policach odbyło się w terminie do dnia 18.11.2010 r. Po tym szkoleniu uzupełniająco dokonywano szkoleń osób przebywających na absencji. Również dokonywano szkoleń po modyfikacji aplikacji*.

(dowód: akta kontroli str. 37, 39, 581)

W listopadzie 2010 roku KPP, na wniosek KWP przeprowadziła m.in. analizę potrzeb sprzętowych w zakresie wyposażenia w sprzęt komputerowy, który miał umożliwiać efektywne wykorzystanie aplikacji e-Posterunek. Komendant KPP w piśmie z 18.11.2010 r., poinformował KWP, m.in. że przeszkolono 13 funkcjonariuszy pionu dochodzeniowo-śledczego. *Z uwagi na problemy sprzętowe*

[28] Zwanym dalej *CDO*.

(komputery o małych parametrach) aplikację e-Posterunek do chwili obecnej, zainstalowano jedynie na 2 komputerach (…).

(dowód: akta kontroli str. 538-539)

W pismach z 7.03.2011 r.[29] oraz 17.03.2011 r.[30] KWP przekazała informacje dotyczące zgłaszania zauważonych błędów w aplikacji e-Posterunek, w tym o umieszczeniu CDO instrukcji dotyczących ww. aplikacji oraz o możliwości korzystania z istniejącego forum na PPW. Informacje i raporty o usterkach w trakcie wdrażania aplikacji e-Posterunek, KPP przekazywała do KWP. Przykładowo 18.06.2012 r. telefonicznie przekazano informację, że aplikacja po instalacji nie uruchamia się na koncie użytkownika (uzyskano odpowiedź umożliwiającą usunięcie problemu); 13.11.2012 r. przekazano telefonicznie oraz pocztą elektroniczną (w tym również do KGP) informację, o braku dostępu do niektórych druków w e-Posterunku – otrzymano odpowiedź, że błąd zostanie naprawiony w nowej wersji aplikacji.

(dowód: akta kontroli str. 482, 566-575)

Sprzęt komputerowy na którym przewidziano zainstalowanie systemu e-Posterunek KPP otrzymała od KWP w Szczecinie w terminach:

- 9.12.2010 r. - Notebook DELL Latitude[31] (1 szt.), na którym pierwszą instalacją aplikacji e-Posterunek była wersja 1.8.4.0 (zainstalowana 7.12.2010 r.),
- 18.05.2011 r. - dostępowe urządzenie mobilne Twinhead Durabook U12C (1 szt.), na którym pierwszą instalacją aplikacji e-Posterunek była wersja 1.8.4.0 (zainstalowana 29.05.2011 r.),
- 27.09.2011 r. – 4 zestawy komputerowe Topadvert 1100S, na których pierwszą instalacją aplikacji e-Posterunek były wersje 1.8.4.0 (zainstalowane 3 i 4.10.2011 r.),
- 6.12.2011 r. - 7 Notebooków Lenovo L520, na 6 pierwszą instalacją aplikacji e Posterunek były wersje 1.8.4.0, a na 1 1.8.8.0 (zainstalowane w okresie 12-14.12.2011 r.),
- 6.06.2012 r. - Mobilny Terminal Przewoźny MTP SUNIT D 10[32] (1 szt. - poprzednio użytkowany przez Oddział Prewencji Policji w Szczecinie), na którym pierwszą instalacją aplikacji e-Posterunek była wersja 2.0.0.3 (zainstalowana 11.06.2012 r.).

Wszystkie zainstalowane aplikacje zostały zaktualizowane do wersji 2.0.0.3. Przekazany sprzęt komputerowy został rozdysponowany bez zbędnej zwłoki, w terminie nie przekraczającym 13 dni od daty otrzymania, z tego pracownicy/funkcjonariusze:

- WK Zespołu Dochodzeniowo - Śledczego KPP otrzymali: Notebooka DELL Latitude, Twinhead Durabook U12C, 7 Notebooków Lenovo L520 oraz 3 zestawy komputerowe Topadvert 1100S,
- Wydziału PiRD KPP otrzymali MTP,
- Zespołu Łączności i Informatyki KPP otrzymali zestaw komputerowy Topadvert 1100S.

Instalacji (aktualizacji) dokonywało 2 pracowników KPP[33] przy wsparciu telefonicznym Wydziału Łączności i Informatyki KWP w Szczecinie.

(dowód: akta kontroli str. 82-87, 88, 91-100)

---

[29] Nr DA-I-0402-60/10 podpisane przez Naczelnika Wydziału Dochodzeniowo – Śledczego KWP.

[30] Nr ŁI-549/11 podpisane przez Naczelnika Wydziału Łączności i Informatyki KWP.

[31] Sprzęt przekazany KWP w Szczecinie przez Wyższą Szkołę Policji w Szczytnie na podstawie umowy użyczenia Nr 5/2010/WŁiOI z dnia 22.11.2010 r., zakupiony ze środków Ministerstwa Nauki i Szkolnictwa Wyższego w ramach Projektu rozwojowego Wyższej Szkoły Policji w Szczytnie „Budowa prototypu Elektronicznego Modułu Procesowego" Nr O R00 0040 08, zwana dalej: *umową użyczenia Nr 5/2010/WŁiOI*. Po upływie czasu użyczenia (18.10.2011 r.) sprzęt został przejęty na stan KWP w Szczecinie, a następnie KPP w Policach.

[32] Dalej: *MPT*.

[33] Zespołu Łączności i Informatyki oraz Zespołu ds. Ochrony Informacji Niejawnych.

Otrzymany sprzęt komputerowy nie był modernizowany w celu użytkowania aplikacji e-Posterunek. MTP wyposażony był m.in. w dysk twardy 40 GB oraz pamięć operacyjną RAM 1 GB DDR SDRAM 400 MHz, tj. podzespoły techniczne niespełniające minimalnych zalecanych wymagań określonych w „Podręczniku administratora aplikacji e-Posterunek2.0", według których minimalną wymaganą konfiguracją sprzętową, niezbędną do uruchomienia i prawidłowego działania aplikacji e-Posterunek były m.in.: dysk twardy 160 GB oraz typ zastosowanej pamięci RAM: DDR2 (667 MHz).

(dowód: akta kontroli str. 88, 91-100 , 559-562)

Administrator systemów teleinformatycznych wyjaśnił, że *nie podejmowano działań w zakresie modernizacji i doposażenia stanowisk dostępowych w celu zapewnienia minimalnych wymagań systemu e-Posterunek, gdyż otrzymany sprzęt przeznaczony do pracy owej aplikacji był zgodny z minimalnymi wymaganiami*. Ponadto wyjaśnił, że sprawa doposażenia MTP *była zgłaszana telefonicznie pracownikom KWP w Szczecinie. Z uzyskanych informacji wynika, iż sprawa rozbudowy urządzeń MTP jest w trakcie realizacji na poziomie KGP w Warszawie i planowana jest rozbudowa owych urządzeń*.

(dowód: akta kontroli str. 542, 543)

W ramach wdrażania systemu e-Posterunek KPP otrzymała z KWP:

- 3 drukarki mobilne w zestawie z dodatkowymi tuszami, z tego otrzymaną 9.12.2010 r. w tym samym dniu przekazano użytkownikowi, otrzymaną 27.09.2011 r. przekazano użytkownikowi 7.10.2011 r. oraz otrzymaną 15.02.2012 r. (HP Office Jet 100) przekazano użytkownikowi[34] 17.04.2012 r. - tj. po 62 dniach od przekazania przez KWP,
- 18.05.2011 r. karta SIM nr 911927(…) na wyposażeniu otrzymanego dostępowego urządzenia mobilnego Twinhead Durabook U12C (w dniu 23.05.2011 r. ww. karta została przyjęta do użytkowania przez asystent w Zespole Dochodzeniowo - Śledczym KPP), w dniu 10.07.2012 r.[35] ww. karta została wymieniona na kartę o numerze 894803(…),
- 1.12.2012 r. aparat cyfrowy Olympus FE 5030[36] (ww. aparat otrzymał 1.12.2010 r. do użytkowania asystent w Zespole Dochodzeniowo - Śledczym KPP).

(dowód: akta kontroli str. 82-87, 88, 91-100, 101-103)

Administrator systemów teleinformatycznych w sprawie rozdysponowania drukarki po 62 dniach od otrzymania wyjaśnił, że *wcześniej nie było wiadomo kto otrzyma sprzęt w postaci stanowiska dostępowego, do którego była ona dedykowana*.

(dowód: akta kontroli str. 542, 544)

Komendant wyjaśnił, że *funkcjonariusz nie używa Durabooka do czynności poza jednostką, a w pokoju posiada możliwość połączenia z siecią za pośrednictwem przewodu* (…) *i nie ma obecnie potrzeby wykorzystania zainstalowanej karty SIM*.

(dowód: akta kontroli str. 42, 43)

Asystent w Zespole Dochodzeniowo - Śledczym KPP wyjaśnił, że *karta SIM dotychczas nie była używana, ponieważ sprzęt nie był wykorzystywany poza budynkiem KPP Police. W siedzibie KPP wykorzystywana jest Policyjna Sieć Transmisji Danych*[37]. Ponadto stwierdził, że *nie ma wiedzy, czy karta była w ogóle aktywowana*.

(dowód: akta kontroli str. 328)

---

[34] Referent w Zespole Dochodzeniowo - Śledczym KPP.
[35] Data przyjęcia przez użytkownika.
[36] Aparat cyfrowy otrzymany przez KWP w Szczecinie na podstawie umowy użyczenia Nr 5/2010/WŁiOI.
[37] Zwaną dalej: PSTD.

W wyniku dokonanych oględzin stwierdzono m.in., że aparat cyfrowy Olympus FE 5030 wykorzystano w 1 sprawie, poza aplikacją e-Posterunek, do sporządzenia dokumentacji fotograficznej stanowiącej załączniki do 3 protokołów oględzin rzeczy (wykonanych w dniach 3, 8 i 10 lutego 2012 r. (łącznie około 50 zdjęć). W pamięci wewnętrznej aparatu stwierdzono 3 zdjęcia wykonane w ramach ww. sprawy.

(dowód: akta kontroli str. 318)

Asystent w Zespole Dochodzeniowo - Śledczym KPP wyjaśnił, że *aparat nie był wykorzystywany do pracy z aplikacją e-Posterunek. Kilkakrotnie uruchomiony był przy okazji prowadzonych czynności celem sprawdzenia jego działania. Działa poprawnie*.

(dowód: akta kontroli str. 330)

Na dzień 12.11.2012 r. w KPP było 11 użytkowników aplikacji e-posterunek, tj. wszyscy funkcjonariusze zatrudnieni byli w WK i wykonywali czynności dochodzeniowo-śledcze[38].

(dowód: akta kontroli str. 82-84, 88, 104-105)

Szkolenia użytkowników aplikacji e-Posterunek rozpoczęto w 2010 r., tj. przed otrzymaniem przez KPP sprzętu komputerowego przeznaczonego do obsługi tej aplikacji. Szkolenia zostały zrealizowane zgodnie z wytycznymi KWP w systemie kaskadowym, tzn. 1 funkcjonariusz z WK, który w założeniu jako koordynator miał przeszkolić pozostałych użytkowników w jednostce, uczestniczył 21.09.2010 r. w szkoleniu w KWP (czas trwania szkolenia ok. 4-5 godzin). Koordynator szkolił następnych użytkowników, w tym w dniach:

- 17, 18 listopada i w grudniu 2010 r. (m.in. 15 i 16) oraz w lipcu 2012 r. – w szkoleniu trwającym ok. 1 godziny udział wzięło 11 funkcjonariuszy WK[39] oraz 2 funkcjonariuszy Wydziału PiRD KPP; na szkoleniu dokonano pokazu aplikacji, omówiono funkcje i jej założenia; prezentacje odbywały się z wykorzystaniem jednego stanowiska (prowadzącego) i nie obejmowały praktycznych ćwiczeń,
- 25.06.2012 r. oraz w lipcu 2012 r. – w szkoleniu trwającym ok. 1 godziny udział wzięło 11 funkcjonariuszy WK; na szkoleniu dokonano pokazu aplikacji oraz przeprowadzono ćwiczenia praktyczne, które odbywały się z wykorzystaniem stanowisk użytkowników.

(dowód: akta kontroli str. 104-105)

Komendant wyjaśnił, że *KPP nie brało udziału przy konsultacjach w trakcie tworzenia systemów SWD i e-posterunek*. Ponadto wyjaśnił, że monitorowanie wprowadzenia systemów SWD i e-Posterunek *prowadziła KWP w Szczecinie poprzez określanie terminów: szkoleń, przydziału i daty odbioru sprzętu niezbędnego do uruchomienia, sporządzenia w przypadku SWD niezbędnych danych jak min. sporządzanie mapy powiatu, sektorów, dzielnic, nadawanie uprawnień. Na szczeblu KPP byłem odpowiedzialny za terminową realizację i wyznaczenie osób do szkolenia*.

(dowód: akta kontroli str. 37, 39-40)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości

Uwagi dotyczące badanej działalności

NIK zwraca uwagę na potrzebę modernizacji MTP, w celu jego dostosowania do minimalnych zalecanych wymagań określonych w „Podręczniku administratora aplikacji e-Posterunek2.0".

[38] Aplikacja e-Posterunek zainstalowana była również na MPT (niewykorzystywana), ponadto szkolenia z obsługi aplikacji odbyli Naczelnik oraz Zastępca Naczelnika WK.

[39] Z tego: 1 odszedł na emeryturę, 2 zostało przeniesionych do Wydziału PiRD KPP.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność kontrolowanej jednostki w zbadanym zakresie.

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

2.1. SWD

Opis stanu faktycznego

Termin oficjalnego wdrożenia SWD w KPP (nie później niż do 31.12.2012 r.) został dotrzymany. SWD, od 17.09.2012 r. (data wdrożenia), stanowi główne narzędzie pracy służby dyżurnej KPP.

(dowód: akta kontroli str. 106-158, 479)

W wyniku oględzin stanowiska służby dyżurnego KPP w zakresie sposobu funkcjonowania SWD ustalono, że:

- w systemie są ewidencjonowane informacje dotyczące zgłoszeń przyjmowanych przez dyżurnych, zdarzeń i interwencji oraz dane o: grafikach służby funkcjonariuszy i dyslokacji służby patrolowej, zarządzanie patrolami;
- istnieje możliwość przekształcenia zdarzenia SWD w wydarzenie KSIP i bezpośredniego przekazania danych miedzy SWD a KSIP;
- istnieje możliwość przeprowadzenia z poziomu SWD sprawdzenia (np. osoby, pojazdu, rzeczy) przez System Poszukiwawczy Policji w KSIP;
- według stanu na dzień 29 listopada 2012 r. w SWD nie była aktywna zakładka *Mapa*;
- zakładki *Zarządzanie akcjami i operacjami* oraz *Zarządzanie blokadami* są aktywne, jednak dotychczas nie były wykorzystywane z powodu braku takiej konieczności;
- według stanu na dzień 10 grudnia 2012 r. była możliwość wygenerowania z systemu, zgodnie z zakresem upoważnień, wszystkich raportów dostępnych w zakładce kreator raportów; przy pierwszej próbie wygenerowania raportu odnotowanych zdarzeń w SWD w dniu 3.12.2012 r. system SWD przestał działać. W kolejnej próbie 10.12.2012 r. wygenerowano ww. raport.
- zakładka *Bieżące komunikaty* była wykorzystywana;
- istnieje możliwość wygenerowania raportu odprawy zawierającego *Protokół z odprawy do służby patrolowej* na dany dzień;
- aktualizacja aplikacji odbywa się w sposób zdalny przez PSTD.

(dowód: akta kontroli str. 106-158)

Pierwsza próba wygenerowania na komputerze na stanowisku dyżurnego raportu odnotowanych zdarzeń w SWD (w dniu 3.12.2012 r.), za okres od dnia 17.09.2012 r. do 3.12.2012 r. zakończyła się niepowodzeniem – system SWD przestał działać („zawiesił się"). W kolejnej próbie (w dniu 10.12.2012 r.) wygenerowano ww. raport.

(dowód: akta kontroli str. 108, 113-114, 120-121)

W KPP, równolegle z SWD, prowadzone są w formie papierowej „Książki odpraw do służby" (3 szt.): służb patrolowo-interwencyjnych, ruchu drogowego oraz dzielnicowych. „Książki odpraw do służby" prowadzone są przez kierowników komórek organizacyjnych Wydziału PiRD i są wykorzystywane do planowania i dyslokacji patroli. Wymóg prowadzenia ww. dokumentów wynika z zarządzeń Komendanta Głównego Policji: Nr 768 z 14.08.2007 r. w sprawie form i metod wykonywania zadań przez policjantów pełniących służbę patrolową oraz koordynacji działań o charakterze prewencyjnym; Nr 609 z 25.06.2007 r. w sprawie sposobu pełnienia służby na drogach przez policjantów; Nr 528 z 6.06.2007 r. w sprawie

form i metod wykonywania zadań przez dzielnicowego i kierownika rewiru dzielnicowych.

(dowód: akta kontroli str. 107, 122, 133, 142, 150, 159-177, 481)

Zapisy odnośnie stanu broni i amunicji służbowej zdeponowanej w magazynie broni, przekazywanej przez policjantów służby dyżurnej są dodatkowo (oprócz zapisu w KPS w SWD) odnotowywane w KPP w papierowej „Książce przebiegu Służby"[40].

(dowód: akta kontroli str. 478)

W KPP podstawowym sposobem przygotowania grafików służb funkcjonariuszy, było ich sporządzenie w aplikacji OpenOffice lub MS Excel przez kierowników poszczególnych komórek organizacyjnych Wydziału PiRD lub WK. Grafiki były drukowane i zatwierdzane przez Komendanta KPP. W SWD grafiki wprowadzone za poszczególne miesiące 4 kwartału 2012 r., nie były aktualizowane i wykorzystywane do dalszych prac z powodu technicznych trudności związanych z nadmiernym rozbudowaniem tej funkcji i dużym stopniem skomplikowania obsługi. W SWD brakowało m.in. możliwości dzielenia służb, np. w przypadku zmiany trybu pracy (przerw w pracy). Stwierdzone w toku kontroli problemy, związane były z prawidłowym obliczeniem bilansu czasu pracy funkcjonariuszy KPP.

(dowód: akta kontroli str. 122, 133-134, 142, 150)

Z przeprowadzonych w KPP anonimowych ankiet 18 użytkowników końcowych aplikacji SWD wynika, że:

- 72% (13 ankietowanych) oceniło, że wprowadzenie aplikacji SWD nie przyczyniło się do usprawnienia ich pracy i podniesienia jej wydajności, 17% (3) oceniło, iż wdrożenie SWD usprawniło pracę i podniosło jej wydajność, pozostałe 11% (2) nie wyraziło opinii,
- 94% (17) wskazało, że wdrożenie SWD nie spowodowało zmniejszenia ilości sporządzanej dokumentacji w formie papierowej (1 nie wyraził opinii),
- 83% (15) oceniło, że ilość i jakość sprzętu komputerowego nie jest wystarczająca do obsługi SWD, pozostałe 17% (3) oceniło, że jest wystarczająca,
- 56% (10) oceniło SWD jako system średni, 28% (5) jako zły, a 17% (3) jako system dobry.

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

- konieczność prowadzenia rejestrów papierowych,
- zbyt mały zakres doskonalenia lokalnego, jedynie w stopniu podstawowym,
- nieodpowiedni sprzęt do pracy z systemem,
- skomplikowanie (złożoność) systemu np. w ramach wykorzystania przy odprawie do służby, natomiast przydatna dla funkcjonariuszy jednostek policji wyższego stopnia (KWP, KSP, KGP) i dla policjantów zajmujących się statystyką,
- małą elastyczność programu skutkującą brakiem możliwości szybkiej modyfikacji danych,
- możliwość wykazania tylko jednej formy pełnienia służby, podczas gdy często funkcjonariusze wykazują ich kilka podczas jednej służby (dotyczy to również zadań centralnych),
- brak panoramicznych monitorów na stanowiskach z zainstalowanym SWD.

(dowód: akta kontroli str. 385-390, 391-426)

Według sporządzonych w toku oględzin raportów czasów reakcji na zdarzenia SWD-R-026, średni czas reakcji w obszarze miejskim wynosił od 0:03:49 do 0:05:18, a w obszarze wiejskim od 0:10:15 do 0:16:27. Według wydruku z systemu

[40] Na podstawie § 11 ust. 2 zarządzenia nr 1173 Komendanta Głównego Policji z dnia 10 listopada 2004 r. w sprawie organizacji służby dyżurnej w jednostkach organizacyjnych Policji (Dz.Urz. KGP Nr 21, poz. 132 ze zm.).

EKSD za miesiąc sierpień 2012 r., średni czas reakcji w obszarze miejskim wynosił 0:07:05, a w obszarze wiejskim 0:15:49.

(dowód: akta kontroli str. 115-116, 126-127, 146-147, 154-155, 576)

Komendant wyjaśnił, że *SWD wykorzystywany jest do sprawowania nadzoru poprzez sprawdzanie czasu reakcji na zdarzenie, sposobu obsługi zdarzenia, przebiegu i aktywności pełnienia służby zadań do realizacji i ewentualnych wydarzeń*. Ponadto wyjaśnił, że *jest prowadzony monitoring czasu reakcji na zdarzenie poprzez dzienne raportowanie i w ten sposób określenie na której służbie czas reakcji jest zbyt długi (np. poprzez min. niezakończenia interwencji) i zwrócenie uwagi odpowiedzialnemu. Wskaźnik czasu reakcji na zdarzenie nie uległ wydłużeniu. Jest on różny z uwagi na ilość zgłoszeń, pozostających w dyspozycji dyżurnego patroli*.

(dowód: akta kontroli str. 38, 40)

Naczelnik Wydziału PiRD KPP wyjaśnił, że system SWD wykorzystywany do sprawowania nadzoru nad podległymi służbami, m.in. przez wykorzystywanie możliwości generowania raportów dotyczących sposobu odprawienia funkcjonariuszy do służby, w tym rodzaju zlecanych zadań.

(dowód: akta kontroli str. 62, 63)

Naczelnik WK wyjaśnił, że system SWD wykorzystywany jest podczas pełnienia dyżurów oficera kontrolnego, w trakcie odprawy funkcjonariuszy wchodzących do służby lub pełniących dyżury zdarzeniowe.

(dowód: akta kontroli str. 64, 65)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność kontrolowanej jednostki w zbadanym zakresie.

2.2. e-Posterunek

Opis stanu faktycznego

W wyniku oględzin sposobu funkcjonowania w KPP e-Posterunku i wykorzystania tej aplikacji przez użytkowników końcowych[41] oraz na podstawie udzielonych wyjaśnień ustalono, że:

- 3 z 11 funkcjonariuszy WK objętych badaniem prowadziło postępowania z wykorzystaniem systemu e-Posterunek; pozostałe osoby nigdy nie używały e-Posterunku, bądź w ograniczonym stopniu próbowały korzystać z aplikacji; łącznie w zakładce lista postępowań znajdowało się 6 postępowań (w tym 2 postępowania u jednego funkcjonariusza i 4 postępowania u kolejnego funkcjonariusza); w zakładce postępowania zakończone: 4 postępowania (prowadzone przez 2 funkcjonariuszy); w zakładce dokumenty niepowiązane: 32 pozycje (u 4 funkcjonariuszy). Stanowiło to 0,3% ogółu 1.242 postępowań przeprowadzonych od 1.12.2011 r. do 1.12.2012 r. przez WK,
- 2 funkcjonariuszy Wydziału PiRD KPP (użytkowników MTP) nie używało e-Posterunku, bądź w ograniczonym stopniu próbowało korzystać z aplikacji m.in. z powodu nieprowadzenia postepowań przygotowawczych oraz z braku możliwości wydrukowania szkiców sytuacyjnych lub kart Mrd-5 (wykorzystywane są w tym celu gotowe druki),
- żaden z użytkowników nie korzystał z aplikacji e-Posterunek poza siedzibą KPP,

[41] Badaniem objęto wykorzystanie aplikacji przez 11 użytkowników z WK, którym przekazano sprzęt komputerowy z zainstalowaną aplikacją e-Posterunek oraz 2 funkcjonariuszy Wydziału PiRD KPP, użytkowników MPT. Przeprowadzono oględziny komputerów i aplikacji oraz testy umiejętności użytkowników w zakresie wytworzenia z wykorzystaniem e-Posterunku podstawowych dokumentów postępowania przygotowawczego.

- 1 z funkcjonariuszy Wydziału PiRD KPP nie był w stanie zalogować się do aplikacji, z uwagi na pojawiający się błąd przy próbie logowania – pojawiał się komunikat o treści „nie można zbudować obiektu sesji”,
- na wszystkich urządzeniach użytkowanych przez funkcjonariuszy WK (11) zainstalowana była wersja 2.0.0.5 aplikacji e-Posterunek, a na 10 z nich dostępna była jednocześnie wersja 1.8.8.0; na urządzeniu mobilnym (MTP) zainstalowana była wersja 2.0.0.3 aplikacji e-Posterunek,
- istnieje funkcja edycji tworzonych w e-Posterunku dokumentów bezpośrednio przed wydrukiem umożliwiająca modyfikację szaty graficznej,
- na 7 komputerach przenośnych oraz na urządzeniu przenośnym MTP, działała funkcja dyktafonu umożliwiająca zapis nagrania na nośniku wskazanym przed uruchomieniem nagrywania, na 1 komputerze przenośnym ww. test zakończył się niepowodzeniem, ww. funkcja nie działała na 3 komputerach stacjonarnych m.in. z powodu braku mikrofonu,
- wg stanu na dzień 7.12.2012 r. nie działały funkcjonalności e-Posterunku dotyczące: możliwości ustanowienia połączenia z SWD, przyjęcia zgłoszenia z e-PUAP[42] oraz połączenia z KSIP,
- aplikacja umożliwia import zdjęć – funkcja dotychczas niewykorzystywana przez użytkowników,
- aplikacja nie umożliwia importu dokumentów zewnętrznych dotyczących prowadzonego postępowania przygotowawczego, sporządzonych przez inne niż KPP podmioty[43] (np. w formacie pdf lub doc),
- aplikacja nie umożliwia weryfikacji niepowtarzalności numeru sprawy ujmowanego w Rejestrze Spraw Dochodzeniowo – Śledczych (RSD).

Z udzielonych przez użytkowników aplikacji wyjaśnień wynika, iż nie korzystają oni z e-Posterunku ponieważ praca w nim jest bardziej skomplikowana i czasochłonna, niż na dotychczas wykorzystywanych szablonach przygotowanych w edytorach tekstu. Prowadzenie spraw trwało zbyt długo, aplikacja działała mało intuicyjnie i miała zbyt dużo zakładek. Funkcjonariusze wyjaśniali, że szablony są im wystarczające do prawidłowego wykonywania czynności służbowych. Otrzymany na potrzeby e-Posterunku sprzęt wykorzystywany jest w głównej mierze poza tą aplikacją, w tym do generowania dokumentów na potrzeby prowadzonych postępowań oraz do dokonywania sprawdzeń w KSIP.

(dowód: akta kontroli str. 178-384, 477)

Przeprowadzone w KPP anonimowe ankiety wśród 21[44] użytkowników końcowych aplikacji e-Posterunek wykazały m.in.,

- 76% (16) oceniło, że wprowadzenie aplikacji e-Posterunek nie przyczyniło się do usprawnienia ich pracy i podniesienia jej wydajności (10% odnotowało usprawnienie pracy i podniesienia jej wydajności, 14% nie wyraziło opinii),
- 71% (15) ankietowanych wskazało, że wdrożenie e-Posterunku nie spowodowało zmniejszenia ilości sporządzanej dokumentacji w formie papierowej (10% odnotowało zmniejszenie ilości sporządzanej dokumentacji w formie papierowej, 19% nie wyraziło opinii),
- 52% (11) ankietowanych oceniło, że ilość i jakość sprzętu komputerowego nie jest wystarczająca do obsługi e-Posterunku (43% oceniło, że ilość i jakość

[42] Elektroniczna Platforma Usług Administracji Publicznej.

[43] Np. postanowień prokuratora o wszczęciu śledztwa, o przedstawieniu zarzutów, wniosków prokuratora o zwolnienie z tajemnicy bankowej, protokołów z posiedzenia Sądu w przedmiocie zwolnienia z tajemnicy bankowej, wniosków prokuratora o zastosowaniu środka zapobiegawczego, opinii biegłych.

[44] Liczba ankietowanych funkcjonariuszy KPP 13, w tym 2 informatyków; ankiety zostały złożone również przez wszystkich (8) użytkowników aplikacji - funkcjonariuszy Komisariatu Policji w Mierzynie.

sprzętu komputerowego jest wystarczająca do obsługi e-Posterunku, 5% nie wyraziło opinii);
– 62% (13) ankietowanych jednoznacznie oceniło e-Posterunek jako zły system, pozostałe 38% oceniło aplikację jako średnią.

W ankietach funkcjonariusze KPP wskazywali w szczególności na następujące problemy związane z funkcjonowaniem tej aplikacji:
– przeprowadzenie szkoleń zbyt wcześnie przed uruchomieniem aplikacji,
– brak drukarek do komputerów,
– mało wydajne komputery (np. MTP nie spełniają minimalnych wymagań sprzętowych aplikacji),
– brak kompatybilności z dostępnymi systemami (KSIP) z możliwością importowania danych,
– system skomplikowany, zbyt dużo zakładek przy wypełnianiu dokumentów, czasochłonność wprowadzania danych do systemu,
– brak funkcji edytowania generowanych druków procesowych.

(dowód: akta kontroli str. 427-434, 435-476)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność kontrolowanej jednostki w zbadanym zakresie.

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

3.1. SWD

Opis stanu faktycznego

Wraz z aplikacją SWD, KPP otrzymała opracowane na szczeblu KGP dokumenty dotyczące zabezpieczenia danych osobowych przetwarzanych w SWD, tj. Politykę bezpieczeństwa SWD oraz Instrukcję zarządzania SWD.

(dowód: akta kontroli str. 486, 586-607)

Oględziny 6 komputerów na których wykorzystywany był system SWD wykazały m.in. że:
- 4 podłączone były do wydzielonej sieci elektrycznej zabezpieczonej bezpiecznikami różnicowymi, a 2 za pośrednictwem centralnego zasilacza awaryjnego UPS,
- były połączone z wewnętrzną siecią PSTD[45] i nie były połączone z internetem,
- każdy użytkownik posiadał swoje indywidualne konto w systemie,
- przy korzystaniu z aplikacji stosowane były mechanizmy kontroli dostępu do przetwarzania danych w postaci kart chipowych i haseł (każdy użytkownik posiadał własną dostępową kartę mikroprocesorową oraz indywidualne hasło dostępu),
- posiadały oprogramowanie antywirusowe zabezpieczające urządzenia komputerowe przed szkodliwym oprogramowaniem,
- wykorzystywane były do obsługi SWD oraz innych aplikacji wykorzystywanych w pracy Policji (np. Osadzony, CEL, KSIP, LEX, SESPOL, OpenOffice).

(dowód: akta kontroli str. 28-29, 488-489, 106-158)

Ustalone nieprawidłowości

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

[45] Policyjna Sieć Transmisji Danych.

Oględziny 6 komputerów przeznaczonych do obsługi SWD wykazały m.in. że:

a) na zestawie komputerowym, w przypadku którego podczas logowania do systemu operacyjnego nie był stosowany mechanizm kontroli dostępu w postaci kart chipowych i haseł[46], w zasadach kont w Windows (ustawień haseł) wyłączone były wymogi odnośnie złożoności haseł; maksymalny okres ważności hasła wynosił 42 dni; minimalna długość hasła ustawiona była na 0 znaków; minimalny okres ważności haseł wnosił 0 dni;
   zgodnie z pkt IV ppkt 2 załącznika do rozporządzenia MSWiA z dnia 29 kwietnia 2004 r., w przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Według pkt VIII ww. załącznika, w przypadku gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
b) na zestawie komputerowym zainstalowanym na stanowisku dyżurnych, założone było 1 konto użytkownika SWD bez ograniczeń (w grupie administratorów)[47], co umożliwiało instalację dodatkowego oprogramowania,
c) na zestawie komputerowym zainstalowanym na stanowisku dyżurnych, zatrzymany był (wyłączony) program antywirusowy (brak ochrony antywirusowej), a na 1 stanowisku funkcjonariusza WK stwierdzono bazę antywirusową z 20.01.2011 r. ;
   zgodnie z pkt III załącznika do rozporządzenia MSWiA z dnia 29 kwietnia 2004 r., system informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
d) w 1 komputerze stacjonarnym (s/n 64882) użytkowanym w Wydziale PiRD, dostęp do ustawień BIOS nie był zabezpieczony hasłem do czego zobowiązywał pkt 9.1. zaleceń KGP z 29 marca 2012 r. [48]

(dowód: akta kontroli str. 28-29, 488-499, 620-623, 625-632)

Administrator systemów teleinformatycznych wyjaśnił: *w związku z dużą ilością obowiązków – pełnienie funkcji w Zespole Łączności i Informatyki* (…) *oraz w Zespole ds. Ochrony Informacji Niejawnych* (…) *nie jestem w stanie regularnie sprawdzać stanu sprzętu i oprogramowania.* (…) *sukcesywnie usuwane są błędy* (…) *związane z konfiguracją zabezpieczeń otrzymanych stanowisk komputerowych zgodnie z „Wytycznymi Biura Łączności KGP nr La 1346/10 z dnia 6.07.2010 r. w sprawie standardów technicznych, użytkowych oraz bezpieczeństwa, stosowanych w Policji w zakresie Informatyki i Łączności*.

(dowód: akta kontroli str. 76, 78-79)

Starszy technik w Zespole Łączności i Informatyki KPP wyjaśnił: *w związku z dużą ilością obowiązków (…) nie jestem w stanie regularnie sprawdzać stanu sprzętu i oprogramowania, reaguję na bieżące zgłoszenia użytkowników i w miarę możliwości usuwam zauważone usterki.* Ponadto wyjaśnił, że *zestaw do Optimus OPTech DP 400 s/n 802.023.998 uszkodzeniu uległ program antywirusowy i aktualnie został on przeinstalowany i zaktualizowany*.

(dowód: akta kontroli str. 70, 71-72)

cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, działalność KPP w zbadanym zakresie.

[46] Zestaw w pokoju nr 134.

[47] W toku oględzin administrator przeniósł użytkownika do grupy użytkowników z ograniczeniami.

[48] „Zalecenia standardów technicznych, użytkowych oraz bezpieczeństwa stosowanych w Policji w zakresie informatyki i łączności" Dyrektora Biura Łączności i Informatyki Komendy Głównej Policji z 29.03.2012 r. (Lj-1321/12), dalej *zalecenia KGP z 29 marca 2012 r.*

3.2. e-Posterunek

Opis stanu faktycznego

W KPP nie sporządzono, a także nie otrzymano od podmiotów zewnętrznych (Komendy Głównej Policji w Warszawie administratora danych osobowych przetwarzanych w aplikacji e-Posterunek lub z Komendy Wojewódzkiej Policji w Szczecinie), dokumentów wymaganych na podstawie art. 36 ust. 1 i 2 ustawy o ochronie danych osobowych oraz § 3 rozporządzenia MSWiA z dnia 29 kwietnia 2004 r., tj. polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych dotyczących aplikacji e-Posterunek.

(dowód: akta kontroli str. 486-487)

Komendant wyjaśnił, że nie opracowano polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, z uwagi iż nie otrzymano ich *od jednostek wyższego szczebla, a administratorem e-Posterunku jako zbioru centralnego jest KGP.* Do *opracowania polityki bezpieczeństwa i instrukcji zarządzania systemem wymagane są dane zawarte w § 4 i 5* rozporządzenia MSWiA z dnia 29 kwietnia 2004 r.

(dowód: akta kontroli str. 38, 40-41)

Oględziny 13 komputerów przeznaczonych do obsługi aplikacji e-Posterunek wykazały m.in. że:

- 2 komputery stacjonarne podłączone były do wydzielonej sieci elektrycznej zabezpieczonej bezpiecznikami różnicowymi, a 1 za pośrednictwem listwy zasilającej z bezpiecznikami,
- 9 komputerów przenośnych i 3 komputery stacjonarne połączone były z wewnętrzną siecią PSTD[49] i nie były połączone z internetem, a MTP miał możliwość połączenia z internetem z wykorzystaniem modemu i karty SIM (wykorzystywano np. do sprawdzeń w systemie KSIP),
- każdy użytkownik posiadał swoje indywidualne konto w systemie,
- przy korzystaniu z aplikacji e-Posterunek stosowane były mechanizmy kontroli dostępu do przetwarzania danych w postaci loginów i haseł,
- 12 komputerów (przenośne i stacjonarne) posiadało oprogramowanie antywirusowe zabezpieczające urządzenia komputerowe przed szkodliwym oprogramowaniem,
- wykorzystywane były m.in. do obsługi aplikacji wykorzystywanych w pracy Policji (np. Osadzony, CEL, KSIP, LEX, SESPOL, OpenOffice).

(dowód: akta kontroli str. 25-27)

Ustalone nieprawidłowości

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

1. W KPP prowadzono postępowania przygotowawcze na 2 komputerach przenośnych i 1 komputerze stacjonarnym, mimo że w KPP nie sporządzono, a także nie otrzymano *Polityki bezpieczeństwa przetwarzania danych osobowych* (…) oraz *Instrukcji zarządzania systemami teleinformatycznymi służącymi do przetwarzania danych osobowych*, dotyczących aplikacji e-Posterunek.

(dowód: akta kontroli str. 25-27)

Przyjęta 15.06.2009 r. w KPP *Polityka bezpieczeństwa przetwarzania danych osobowych w KPP Police i w Komisariacie Policji w Mierzynie*, nie była uaktualniona o system SWD i aplikację e-Posterunek.

(dowód: akta kontroli str. 490-537)

[49] Policyjna Sieć Transmisji Danych.

Komendant wyjaśnił m.in., że *nie uaktualniono „Polityki bezpieczeństwa …", ponieważ opracowano osobną politykę bezpieczeństwa dla systemu SWD, jednocześnie aplikacje SWD i e-Posterunek są aplikacjami centralnymi, a KPP w Policach jest administratorem lokalnym*. Ponadto wyjaśnił, że *Komendant KPP w Policach nie jest administratorem danych osobowych żadnego zbioru danych w formie informatycznej, nie wdrożył żadnej instrukcji zarządzania*.

(dowód: akta kontroli str. 38, 41, 80-81)

Pełnomocnik ds. Informacji Niejawnych w KPP wyjaśnił, że KPP nie prowadzi i nie stosuje „Polityki bezpieczeństwa …" oraz „Instrukcji zarządzania …." z uwagi na to, że aplikacja e-Posterunek jest centralnym zbiorem, którego administratorem jest Komendant Główny Policji. Ponadto wyjaśniła, że system SWD i aplikacja e-Posterunek nie są zaewidencjonowane w wykazie zbiorów danych osobowych przetwarzanych w KPP z uwagi na to, że ww. zbiory danych osobowych nie są utworzone przez administratora danych osobowych KPP, są to centralne zbiory Komendy Głównej Policji.

(dowód: akta kontroli str. 66, 67)

Administrator systemów teleinformatycznych wyjaśnił, że administratorem danych osobowych przetwarzanych w aplikacji e-Posterunek jest Komendant Główny Policji. *Z uwagi na przystosowywanie następnej wersji aplikacji e-Posterunek do współpracy z programami zewnętrznymi dostępowymi – centralnymi (KSIP, CEL) przedmiotowa dokumentacja jest aktualnie opracowywana na szczeblu KGP i zostanie w przyszłości wdrożona*. Ponadto wyjaśnił, że *„Polityka bezpieczeństwa danych osobowych w KPP w Policach i w KP w Mierzynie" ma zastosowanie wyłącznie do zbiorów danych osobowych, których administratorem jest Komendant KPP w Policach*.

(dowód: akta kontroli str. 76, 78)

W wyniku oględzin ustalono, że z wykorzystaniem 3 niespełniających wszystkich wymogów w zakresie zabezpieczenia przed nieuprawnionym dostępem komputerach, w tym 2 przenośnych (brak zabezpieczenia kryptograficznego; brak zasad definiowania i zmiany haseł do e-Posterunku; brak hasła w BIOS; na 1 komputerze przenośnym: aktualizacja bazy wirusów z 28.02.2012 r. oraz hasło logowania do systemu operacyjnego składające się z 6 cyfr; brak sporządzania kopii zapasowych), prowadzono 6 postępowań przygotowawczych w ramach których przetwarzano dane osobowe osób będących uczestnikami tych postepowań. Działanie to było niezgodne z art. 36 ust. 1 ustawy o ochronie danych osobowych oraz załącznikiem do rozporządzenia MSWiA z dnia 29 kwietnia 2004 roku.

(dowód: akta kontroli str. 25-27, 192-193, 273-274, 318-319)

2. Oględziny 13 komputerów przeznaczonych do obsługi aplikacji e-Posterunek wykazały m.in. że:

a) na 9 komputerach przenośnych[50] w zasadach kont w Windows (ustawień haseł) wyłączone były wymogi odnośnie złożoności haseł; maksymalny okres ważności hasła wynosił 42 dni; minimalna długość hasła ustawiona była na 0 znaków; minimalny okres ważności haseł wnosił 0 dni;
   Zgodnie z pkt IV ppkt 2 załącznika do rozporządzenia MSWiA z dnia 29 kwietnia 2004 r., w przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. W 3 przypadkach ustawione hasło logowania nie zawierało co najmniej 8 znaków, co było niezgodne z pkt VIII załącznika do rozporządzenia MSWiA z dnia 29 kwietnia 2004 r.,
b) na MTP oraz na 3 komputerach przenośnych (w tym na 2 użytkowanych przez koordynatora wdrażania systemu e-Posterunek) założone były 4 konta

[50] Podczas logowania do systemu operacyjnego zainstalowanego na MPT wymagana była karta mikroprocesorowa.

użytkowników bez ograniczeń (w grupie administratorów)[51], co umożliwiało instalację dodatkowego oprogramowania.

c) na MTP nie było zainstalowanego programu antywirusowego, na 7 komputerach przenośnych aktualizacji bazy wirusów dokonano ponad 5 miesięcy przed 26.11.2012 r. (datą przeprowadzenia ostatnich oględzin), w tym w 4 przypadkach aktualizacji dokonano według stanu na 5.12.2011 r., w pozostałych przypadkach odpowiednio na: 22.11.2011 r., 28.02.2012 r. i 22.06.2012 r.;
   zgodnie z pkt III załącznika do rozporządzenia MSWiA z dnia 29 kwietnia 2004 r., system informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
d) na żadnym z komputerów nie były zainstalowane aplikacje szyfrujące, umożliwiające stosowanie kryptograficznych metod ochrony danych, co było niezgodne z pkt V i XIII załącznika do rozporządzenia MSWiA z dnia 29 kwietnia 2004 r. (aktywne były: porty usb (we wszystkich komputerach) oraz porty bluetooth i WiFi w 9 komputerach przenośnych[52]),
e) w żadnym z komputerów nie było ustawione hasło w BIOS, wymagane do wejścia do BIOS (np. w celu zmiany konfiguracji), do czego zobowiązywał pkt 9.1. zaleceń KGP z 29 marca 2012 r.,
f) na wszystkich komputerach zalogowanie do e-Posterunku możliwe było na podstawie hasła odpowiadającego loginowi użytkownika (6 cyfr)[53]; aplikacja nie wymuszała regularnej zmiany hasła dostępowego, ani nie wymuszała na użytkowniku zastosowania w haśle konkretnej ilości znaków, stosowania wielkich/małych liter lub znaków specjalnych[54], co nie spełniało wymogów określonych w pkt IV ppkt 2 oraz pkt VIII załącznika do rozporządzenia MSWiA z dnia 29 kwietnia 2004 r.,
g) z aplikacji e-Posterunek nie były sporządzane kopie zapasowe, co było niezgodne z pkt IV ppkt 3 załącznika do rozporządzenia MSWiA z dnia 29 kwietnia 2004 roku.

(dowód: akta kontroli str. 25-27, 620-623, 625-632)

Administrator systemów teleinformatycznych wyjaśnił: *KPP otrzymała do pracy sprzęt z wgranym systemem Windows i częścią oprogramowania. Należało tylko zainstalować oprogramowanie e-Posterunek i w związku z koniecznością jak najszybszego wydania komputerów użytkownikom skupiono się tylko na założeniu kont i wgraniu oprogramowania. W związku z tym nie sprawdzano pełnego stanu zabezpieczeń (…) W związku z dużą ilością obowiązków – pełnienie funkcji w Zespole Łączności i Informatyki (…) oraz w Zespole ds. Ochrony Informacji Niejawnych (…) nie jestem w stanie regularnie sprawdzać stanu sprzętu i oprogramowania. (…) sukcesywnie usuwane są błędy (…) związane z konfiguracją zabezpieczeń otrzymanych stanowisk komputerowych zgodnie z „Wytycznymi Biura Łączności KGP nr La 1346/10 z dnia 6.07.2010 r. w sprawie standardów technicznych, użytkowych oraz bezpieczeństwa, stosowanych w Policji w zakresie Informatyki i Łączności*.

(dowód: akta kontroli str. 76, 78-79)

Starszy technik w Zespole Łączności i Informatyki KPP wyjaśnił: *KPP otrzymała do pracy sprzęt z wgranym systemem i częścią oprogramowania. W związku z koniecznością jak najszybszego wydania komputerów użytkownikom skupiono się*

[51] Na 2 komputerach przenośnych funkcjonariuszy WK (w toku oględzin 21.11.2012 r. administrator dokonał zmiany uprawnień użytkownika na konto z ograniczeniami - standardowy) oraz na MPT funkcjonariusz w Wydziale PiRD.

[52] Komputery stacjonarne nie były wyposażone w porty bluetooth i WiFi.

[53] Użytkownicy nie zmienili swojego hasła od daty pierwszego logowania do aplikacji.

[54] Przeprowadzony test w toku oględzin wykazał, że zalogowanie się do aplikacji e-Posterunek możliwe było na podstawie przykładowego loginu i hasła: 12345.

tylko na założeniu kont oraz wgraniu oprogramowania, a nie sprawdzano pełnego stanu zabezpieczeń. (…) W związku z dużą ilością obowiązków (…) *nie jestem w stanie regularnie sprawdzać stanu sprzętu i oprogramowania, reaguję na bieżące zgłoszenia użytkowników i w miarę możliwości usuwam zauważone usterki.* Ponadto wyjaśnił, że *wszystkie notebooki Lenovo L520 miały zainstalowane oprogramowanie Dr.WEB, v7, który wg. mojej wiedzy miały aktualizować się automatycznie z serwerów w sieci PSTD, użytkownicy nie zgłaszali mi iż bazy są nieaktualne, (…). Do aktualizacji programów Dr.Web v.7 zainstalowanych na laptopach Lenovo utworzono w bieżącym miesiącu lokalny serwer w KWP Szczecin i po skonfigurowaniu programu – wpisaniu adresu serwera aktualizują się przez ww. serwer*. Ponadto, w sprawie haseł dostępowych do aplikacji e-Posterunek wyjaśnił, że aplikacja *była instalowana jednocześnie na wszystkich komputerach i aby nie pomylić się przy pierwszym uruchomieniu zastosowano hasła tożsame z loginem i łatwe do zapamiętania dla mnie i użytkownika, gdyż użytkownicy nie od razu korzystali z ww. aplikacji, zasadę taką stosuje się też w innych programach jednak przy pierwszym uruchomieniu programy wymuszają zmianę hasła przez użytkownika, jako że nie byłem na żadnym szkoleniu z ww. aplikacji nie wiedziałem, iż ten program nie wymusza zmiany hasła przy pierwszym uruchomieniu ani nie umożliwia zmiany hasła z poziomu użytkownika*.

(dowód: akta kontroli str. 70, 71-72)

Pismem z 13 grudnia 2012 r. kontrolujący przekazał Komendantowi, na podstawie przepisów art. 51 ust. 4 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[55], informację o nieprawidłowościach związanych z wdrożeniem w KPP aplikacji e-Posterunek, tj. bez wymaganej dokumentacji (polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych) oraz o przypadkach wykorzystywania aplikacji e-Posterunek na nieprawidłowo zabezpieczonym przed nieuprawnionym dostępem sprzęcie komputerowym.

(dowód: akta kontroli str. 483-484)

Komendant odpowiadając w piśmie z 19.12.2012 r. poinformował m.in., że w rozdziale VII „Zaleceń dotyczących standardów technicznych, użytkowych oraz bezpieczeństwa stosowanych w Policji w zakresie informatyki i łączności" zatwierdzonych 29.03.2012 r. (wpłynęły do KPP 5.04.2012 r.) ujęto m.in., że użytkownik sprzętu komputerowego zobowiązany jest do ochrony i nieudostępniania informacji przechowywanych na komputerze osobom do tego nieuprawnionym. (…) *W celu stosowania się do zaleceń wydałem polecenie o ponownym zapoznaniu się z dokumentem* (…).

(dowód: akta kontroli str. 68-69, 485)

Zastępca Komendanta Wojewódzkiego Policji w Szczecinie w piśmie z 21.12.2012 r.[56] zwrócił się do Komendantów Powiatowych/Miejskich Policji o wstrzymanie wykorzystywania aplikacji e-Posterunek do prowadzenia postepowań przygotowawczych na rzeczywistych danych. Z-ca Naczelnika Wydziału Łączności i Informatyki KWP poinformował Komendantów Powiatowych/Miejskich Policji (pismo z 3.01.2013 r. nr ŁI-2112/2012) o opracowaniu przez Biuro Łączności i Informatyki KGP procedury usunięcia danych z aplikacji e-Posterunek oraz polecił usuniecie z tej aplikacji postępowań przygotowawczych prowadzonych na rzeczywistych danych.

(dowód: akta kontroli str. 584, 585)

[55] Dz.U. z 2012 r., poz. 82, zwanej dalej *ustawą o NIK*.
[56] L.dz. DA-I-60/2010/RL.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, działalność 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 o NIK, wnosi o:

1. Wydawanie upoważnień dostępu do SWD po zapoznaniu użytkowników z dokumentami dotyczącymi ochrony danych osobowych przetwarzanych w tym systemie.
2. Dokonanie przeglądu sprzętu informatycznego obsługującego w KPP aplikację SWD nieobjętego kontrolą NIK, w zakresie sposobu zabezpieczenia przed nieuprawnionym dostępem.

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 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 pokontrolnych 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
Jarosław Staniszewski
doradca ekonomiczny

Dyrektor

..... *podpis*

..... *podpis*