NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie

LSZ – 4101-26-03/2012
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

Jarosław Staniszewski, doradca ekonomiczny, upoważnienie do kontroli nr 83634 z dnia 30 października 2012 r.

Radosław Kropiowski, główny specjalista kontroli państwowej, upoważnienie do kontroli nr 83641 z dnia 13 listopada 2012 r.

Tomasz Cyranka, główny specjalista kontroli państwowej, upoważnienie do kontroli nr 85165 z dnia 4 grudnia 2012 r.

(dowód: akta kontroli str. 1-6)

Jednostka kontrolowana

Komenda Miejska Policji w Szczecinie[1], ul. Kaszubska 35.

Kierownik jednostki kontrolowanej

Inspektor Jacek Wolf, Komendant Miejski Policji w Szczecinie[2], od dnia 18 lutego 2010 r.

(dowód: akta kontroli str. 7)

II. Ocena kontrolowanej działalności

1. System Wspomagania Dowodzenia[3].

Ocena ogólna

Najwyższa Izba Kontroli ocenia pozytywnie wdrożenie i funkcjonowanie SWD w KMP w Szczecinie.

Uzasadnienie oceny ogólnej

Wyniki kontroli wykazały, że SWD był podstawowym narzędziem pracy służby dyżurnej w KMP. W systemie były rejestrowane wymagające tego zgłoszenia, zdarzenia oraz czynności związane z reakcją Policji. Na bieżąco była wprowadzana dyslokacja służb patrolowo-interwencyjnych. W KMP nie wprowadzano do SWD grafików służb policjantów, ale nie stwierdzono aby wpłynęło to negatywnie na wykonywanie zadań Policji.

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. KMP nie otrzymała wytycznych w tym zakresie od jednostek organizacyjnych

[1] Dalej *KMP* lub *Komenda*.
[2] Dalej *Komendant*.
[3] Dalej *SWD*.

wyższego szczebla, tj. od Komendy Wojewódzkiej Policji w Szczecinie[4] i Komendy Głównej Policji[5].

Otrzymane przez KMP komputery i drukarki przeznaczone do obsługi e-Posterunku zostały bez zbędnej zwłoki przekazane komórkom organizacyjnym Komendy i funkcjonariuszom realizującym zadania służby dochodzeniowo-śledczej. Wykorzystywano je głównie do prowadzenia postępowań przygotowawczych z wykorzystaniem standardowych edytorów tekstu oraz dokonywania sprawdzeń w systemach informatycznych Policji.

Stwierdzona nieprawidłowość polegała na niezabezpieczeniu części sprzętu informatycznego przed nieuprawnionym dostępem.

III. Opis ustalonego stanu faktycznego

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

1.1. SWD.

Opis stanu faktycznego

W KMP na podstawie decyzji z 24.11.2011 r.[6] wyznaczono lokalnych administratorów SWD. Poza tą decyzją nie opracowano w Komendzie żadnych innych aktów prawnych ani procedur dotyczących zasad organizacji pracy komórek organizacyjnych Komendy z wykorzystaniem SWD.

(dowód: akta kontroli str. 13-15, 101-103, 330)

Komendant wyjaśnił, że inicjatywa w zakresie wdrożenia SWD należała do zespołu ds. wdrożenia i uruchomienia SWD w jednostkach organizacyjnych Policji województwa zachodniopomorskiego powołanego decyzją nr 212/11 Komendanta Wojewódzkiego Policji w Szczecinie z 18.08.2011 r. Komendant KMP realizował zadania wynikające z tej decyzji oraz zalecenia wypływające z KWP.

(dowód: akta kontroli str. 327, 330)

Komendant 9.05.2012 r. wystąpił do Naczelnika Wydziału Łączności i Informatyki KWP[7] o zakup na potrzeby stanowisk systemu SWD, 40 sztuk komputerów klasy PC oraz 6 sztuk przełączników sieciowych do sieci.

(dowód: akta kontroli str. 336)

Komenda poza dwoma monitorami zainstalowanymi w Sztabie Policji[8], które miały służyć do obsługi mapy w SWD (przekazanymi przez KWP 22.05.2012 r.), nie otrzymała żadnego sprzętu dedykowanego do SWD.

(dowód: akta kontroli str. 47)

Instalacja oprogramowania SWD została przeprowadzona w Komendzie w październiku 2011 r. przez funkcjonariuszy i pracowników Referatu Łączności i Informatyki[9]. System zaczął funkcjonować od 21.11.2011 r. Aktualizacja aplikacji odbywała się w sposób zdalny przez Policyjną Sieć Transmisji Danych[10]. W związku z wdrażaniem SWD funkcjonariusze i pracownicy RŁiI zwiększyli pamięć RAM od 256 MB do 1 GB na 28 stanowiskach (11 w nadzorowanych Komisariatach i 17 w Komendzie).

(dowód: akta kontroli str. 48-53, 101, 352-357, 358)

---

4 Dalej *KWP*.
5 Dalej *KGP*.
6 Nr 122/2011.
7 Dalej *WŁiI KWP*.
8 Dalej SzP.
9 Dalej RŁiI.
10 Dalej *PSTD*.

Szkolenia z zakresu SWD były prowadzane od X 2011 r. do I 2012 r. przez 2 funkcjonariuszy Komendy (ze SzP i Wydziału Prewencji[11]) oraz 2 funkcjonariuszy KWP, którzy ukończyli pięciodniowy kurs trenerów w Ośrodku Szkolenia Policji w Łodzi z siedzibą w Sieradzu[12]. Przeszkolonych zostało 82 osoby, z tego: 3 osoby przez 3 dni[13], 20 osób przez 2 dni[14] (18 ze SzP, 2 z Wydziału Ruchu Drogowego[15]), 59 przez 1 dzień. Szkolenia zostały zrealizowane na sprzęcie komputerowym z zainstalowaną szkolną wersją SWD.

(dowód: akta kontroli str. 73-91)

W Komendzie był wykorzystywany system raportowania o usterkach w funkcjonowaniu oprogramowania SWD, który został opracowany w pierwszym kwartale 2012 r. przez KGP[16]. 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[17] 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. 580-582)

Wg stanu na 20.11.2012 r. oprogramowanie SWD zostało zainstalowane na 32 stacjach dostępowych w Komendzie, tj. w: SzP 10, Zespole Dyżurnych (znajdującym się w budynku Sztabu) 2; WP 8, Wydziale Kryminalnym[18] 3, WRD 4, Referacie Skarg i Wniosków[19] 2; RŁiI 3 oraz na 46 stacjach dostępowych znajdujących się w nadzorowanych przez Komendę 5 Komisariatach.

(dowód: akta kontroli str. 48-53)

Docelowymi użytkownikami oprogramowania SWD w Komendzie było: w SzP – 49 osób[20]; WP 30 osób[21]; WRD 12 osób[22]; RŁiI: 3 osoby; RSiW: 3 osoby. Na poziomie nadzorowanych komisariatów[23]: 77 osób. W złożonych wyjaśnieniach Komendant dodatkowo stwierdził, że SWD jest podstawowym narzędziem pracy dyżurnego jednostki organizacyjnej policji, natomiast odpowiedzialność za patrole, które należy odpowiednio skonfigurować i zalogować do SWD, a następnie rozliczyć po zakończonej służbie została nałożona na innych funkcjonariuszy WP i nadzorowanych Komisariatów, tj. kierownictwo, kierowników ogniw, specjalistów, ds. organizacji służby - 40 osób na poziomie Komendy i 15 na poziomie Komisariatów.

(dowód: akta kontroli str. 333-334)

Wszystkie osoby będące użytkownikami SWD zostały zapoznane z dokumentami dotyczącymi ochrony danych osobowych przetwarzanych w tym systemie, w tym z *Polityką bezpieczeństwa systemu wspomagania dowodzenia jednostek organizacyjnych Policji – poziom wysoki*[24], oraz *Instrukcją zarządzania systemem*

---

[11] Dalej *WP*.
[12] Szkolenie dwa dni w formie praktycznej na sprzęcie z zainstalowanym oprogramowanie, pozostałe 3 dni, z powodu awarii sprzętu w formie teoretycznej.
[13] 3 x 8 godzin.
[14] 2 x 8 godzin.
[15] Dalej *WRD*.
[16] Pismo Zastępcy Komendanta Głównego Policji z 28.03.2012 r. (wpływ do Komendy 02.04.2012 r.)
[17] Dalej *PPW*.
[18] Dalej *WK*.
[19] Dalej *RSiW*.
[20] Zespół Dyżurnych: 10 osób, Zespół – Stanowisko Kierowania: 25 osób, rezerwa kadrowa: 4 osoby, pracownicy cywilni: 10 osób. Dodatkowo w SzP na oprogramowaniu SWD pracowało 9 osób, pracowników Wojewódzkiego Centrum Powiadamiania Ratunkowego Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie.
[21] Kierownictwo oraz kierownicy ogniw i referatów, specjaliści.
[22] Kierownictwo oraz kierownicy ogniw, specjaliści.
[23] Kierownictwo, dyżurni, zastępcy dyżurnych, dzielnicowi, kierownicy ogniw.
[24] Dalej *Polityka bezpieczeństwa SWD*.

teleinformatycznym przetwarzającym dane osobowe – system wspomagania dowodzenia jednostek organizacyjnych Policji – poziom wysoki[25].

(dowód: akta kontroli str. 38-46)

Ustalone nieprawidłowości

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

Uwagi dotyczące badanej działalności

Ustalono, że 36 ze 129 osób – funkcjonariuszy Komendy (bez nadzorowanych Komisariatów) posiadających upoważnienie do dostępu do SWD, nie odbyło szkolenia w zakresie obsługi SWD.

(dowód: akta kontroli str. 39-45, 73-91)

W zatwierdzonej przez Komendanta Głównego Policji Polityce bezpieczeństwa SWD w pkt. 1.7 m.in. określono, że przed uzyskaniem dostępu do danych osobowych SWD wszyscy użytkownicy muszą zostać upoważnieni do przetwarzania danych osobowych i przeszkoleni w zakresie wykonywania czynności zapewniających ochronę danych osobowych. W pkt 3 Polityki m.in. stwierdzono, że wymagania bezpieczeństwa danych osobowych są realizowane poprzez zapewnienie przetwarzania danych osobowych w systemie SDW tylko przez osoby przeszkolone i upoważnione.

(dowód: akta kontroli str. 596)

Komendant wyjaśnił, że w jego ocenie elementem niezbędnym do wydania upoważnienia do dostępu do SWD jest przeszkolenie w zakresie wykonywania czynności zapewniających ochronę danych osobowych, a nie szkolenie techniczne z zakresu obsługi aplikacji SWD.

(dowód: akta kontroli str. 96, 99, 101-103)

W Polityce bezpieczeństwa SWD 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. 596)

Komendant wyjaśnił, że SWD został wdrożony w dniach 14-16.11.2011 r. przez Zespół Wdrożeniowych KGP, a uruchomiony 21.11.2011 r. W tym okresie trwały już szkolenia, jednak z związku z nagłą awarią systemu GEMC3, nastąpiła konieczność wcześniejszego wprowadzenia do użytku SWD. Tym samym szkolenia jeszcze trwały, sam system został już uruchomiony. W praktyce mogło to doprowadzić do tego, że wielu użytkowników, a w szczególności dyżurni KMP/KP, którzy nie posiadali upoważnienia do dostępu do SWD, zostaliby pozbawieni możliwości zalogowania do systemu i wykonywania swoich czynności służbowych. Wobec powyższego wystąpiono w okresie bezpośrednio poprzedzającym uruchomienie SWD o nadanie uprawnień dla planowanych użytkowników (w pierwszej kolejności dla funkcjonariuszy służby dyżurnej, rezerwy kadrowej, kierowników komórek organizacyjnych). Jak się później okazało z wnioskami o nadanie uprawnień wystąpiono także do osób, które faktycznie nie korzystały z systemu.

(dowód: akta kontroli str.104-104[1])

Ocena cząstkowa

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

[25] Dalej *Instrukcja zarządzania SWD*.

1.2. e-Posterunek.

Opis stanu faktycznego

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

(dowód: akta kontroli str.213-215, 217-269)

Komendant wyjaśnił, że wynikało to z braku poleceń jednostek wyższego szczebla, do wydania przez KMP decyzji o wprowadzeniu aplikacji e-Posterunek do użytku.

(dowód: akta kontroli str. 586, 588)

Komenda nie była informowana o terminach wdrażania aplikacji e-Posterunek. W piśmie KWP z 13.09.2009 r.[26] m.in. stwierdzono, że: *„będący obecnie na stanach jednostek sprzęt jest niewystarczający zarówno ilościowo jak i technicznie do zaspokojenia pełnych potrzeb. Nie mniej mając na uwadze wyznaczony przez KGP termin wprowadzania aplikacji, rozpoczęcie prac musi nastąpić na bazie posiadanego sprzętu".* W piśmie tym nie została jednak wskazana data (dzień, miesiąc, rok) wprowadzenia aplikacji.

(dowód: akta kontroli str.329, 331, 213-214, 217-219)

Pierwsza instalacja aplikacji e-Posterunek odbyła się na przełomie III/IV kwartału 2010 r. przez pracowników RŁiI na dotychczas posiadanym przez Komendę sprzęcie. Komendant wyjaśnił, że ze względu na okres jaki upłynął od tej instalacji nie jest możliwie ustalenie kiedy (data dzienna), na ilu jednostkach i która wersja aplikacji została zainstalowana.

(dowód: akta kontroli str. 327, 331, 335)

Instalacja aplikacji e-Posterunek na sprzęcie dedykowanym do tej aplikacji, wg stanu na 31.12.2012 r., następowała: w grudniu 2011 r. (wersja 1.8.8.0) na 82 notebookach Lenowo, w tym: dla 3 PG, 3 dla WK, 1 dla RŁiI, reszta dla nadzorowanych Komisariatów; w maju 2011 r. (wersja 1.8.5.0) na 14 dostępowych urządzeniach mobilnych Twinhead Durabook U12C, w tym 1 dla WRD, 1 dla WK, pozostałe dla nadzorowanych Komisariatów; we wrześniu 2011 r. (wersja 1.8.8.0) na 31 zestawach komputerowych Topadvert 1100S, w tym 2 dla PG, 1 dla WK, pozostałe dla nadzorowanych Komisariatów; w marcu 2011 r. (wersja 1.8.5.0) na 2 zestawach komputerowych Aplast (dla Komisariatu Szczecin Dąbie); październiku 2012 r. (wersja 2.0.0.4) na 14 Mobilnych Terminalach Przewoźnych MTP Sunit d10, z których 1 były przeznaczony Komisariatu Szczecin Śródmieście, a 13 dla WRD[27].

(dowód: akta kontroli str. 64-72)

Komendant wyjaśniając czy w przypadkach, w których zainstalowano wersje oprogramowania e-Posterunek 1.8.8.0 i 1.8.5.0 planuje się aktualizację oprogramowania stwierdził, że obecnie instalowana jest nowa wersja aplikacji 2.0.0.8. Nie ma możliwości zaktualizowania poprzednich wersji do wersji obecnej. Nową należy zainstalować od początku, co zajmuje ok. 1,5 godziny. RŁiI nie prowadzi wykazu wersji oprogramowania ze wskazaniem nr ewidencyjnego Stanowiska Dostępowego oraz daty jego instalacji, gdyż nie było w tym zakresie wytycznych lub poleceń z jednostek nadrzędnych, co do sposobu dokumentowania instalowania nowej wersji oprogramowania.

(dowód: akta kontroli str. 327, 335)

Zapotrzebowanie na zakup sprzętu dedykowanego pod aplikację e-Posterunek zostało przekazane przez kierownika RŁiI Naczelnikowi Wydziału Dochodzeniowo-Śledczego KWP przy piśmie z 11.10.2010 r. Wyszczególniono w nim 85

[26] DA-I-0402-60/10/AB dotyczącym prac związanych z wdrożeniem aplikacji e-Posterunek.
[27] Na 31.12.2012 r. 1 uszkodzony terminal, 1 terminal znajdował się w rozbitym pojeździe.

komputerów stacjonarnych, w tym 2 dla WK i 2 dla PG; 47 komputerów przenośnych, w tym 7 dla WK, 2 dla PG; 76 drukarek stacjonarnych, w tym 2 dla WK, 5 dla PG; 43 drukarki przenośne, w tym: 3 dla WK, 2 dla PG.

(dowód: akta kontroli str.335, 338-339)

Komenda otrzymała 150 szt. następującego sprzętu komputerowego dedykowanego do aplikacji e-Posterunek: 21.03.2011 r. 2 szt. zestawu komputerowego Aplast, przekazane do Komisariatu Szczecin Dąbie; 19.05.2011 r. 14 szt. notebooków - dostępowych urządzeń mobilnych Twinhead Durabook U12C, w tym 1 dla WK i 1 dla WRD, pozostałe dla nadzorowanych Komisariatów; 14.07.2011 r. 2 notebooki HP 550, które zostały przekazane do Komisariatu Szczecin Dąbie; 21.09.2011 r. 31 zestawów komputerowych Topadvert 1100S, z których 2 przekazano do PG, 1 do WK, a pozostałe do nadzorowanych komisariatów; 19.10.2011 r. 9 szt. notebooków HP Probook 6560b wraz aparatem cyfrowym Olympus TG-310, przekazane do Komisariatu Szczecin Dąbie; 7.12.2011 r. 75 notebooków Lenovo L520, przekazanych nadzorowanym Komisariatom; 7.12.2011 r. 7 notebooków Lenovo L520, które zostały przekazane do PG (3 szt,), WK (3 szt.) i 1 do RŁiI; 22.12.2011 r. 10 szt. notebooków Dell Latitude E5510, przekazanych nadzorowanym Komisariatom.

(dowód: akta kontroli str.54-62)

Komenda do obsługi aplikacji e-Posterunek otrzymała 13 drukarek, tj. 22.12.2010 r. 10 szt. HP Office Jet H470 w zestawie z dodatkowymi tuszami, przekazane do nadzorowanych Komisariatów; 23.09.2011 r. 1 szt. drukarki HP Office Jet H470 w zestawie z dodatkowymi tuszami, przekazana do RŁiI; 22.02.2012 r. 2 szt. drukarki HP Office Jet H470 w zestawie z dodatkowymi tuszami, z tego: 1 dla RŁiI i 1 dla Komisariatu Szczecin Śródmieście.

(dowód: akta kontroli str.62-63)

Powyższy sprzęt został rozdysponowany bez zbędnej zwłoki w okresie do 1 miesiąca od daty przyjęcia przez Komendę.

(dowód: akta kontroli str.54-63)

Kierownik Referatu Dochodzeniowo-Śledczego WK oświadczył, że system raportowania o usterkach i błędach w działaniu aplikacji e-Posterunek polegał na tym, że od czerwca 2010 r. w sieci PSTD w Centrum Dystrybucji Oprogramowania wskazane były adresy do prowadzenia takiej korespondencji. Natomiast od 1 marca 2011 r. utworzono portal Policyjna Platforma Wdrożeniowa również dostępna w sieci PSTD, gdzie błędy, usterki itp. miały być zgłaszane na forum. Jednocześnie koordynator wojewódzki również za naszym pośrednictwem gromadził takie dane z jednostek podległych.

(dowód: akta kontroli str.214)

KMP informowała KWP o wykorzystaniu aplikacji e-Posterunek w odpowiedzi na pisma KWP z 15.02.2011 r., 18.02.2011 r., 01.08.2011 r., 09.05.2012 r., 23.10.2012 r.

(dowód: akta kontroli str.251-322)

Kierownik Referatu Dochodzeniowo-Śledczego WK oświadczył, że za początek wdrażania w Komendzie aplikacji e-Posterunek należy przyjąć dzień 14.09.2010 r., kiedy to wpłynęło pismo nr DA-I-0402-60/10/AB z dnia 13 września 2010 r. z Wydziału Dochodzeniowo – Śledczego KWP, w którym poinformowano, że trwają pracę nad wdrożeniem aplikacji do użytku dla policjantów prowadzących postępowania przygotowawcze. Według założeń w celu realizacji tego przedsięwzięcia planowano przeprowadzenie cyklu szkoleń dla maksymalnie 2-3 pracowników pionów dochodzeniowo – śledczych z poszczególnych jednostek.

Szkolenia miały dotyczyć obsługi aplikacji. Dla Komendy i podległych jej komisariatów takie szkolenie odbyło się w KWP dnia 21.09.2010 r. Podczas szkolenia przedstawiono założenia, demonstrowano sposób działania, opisano podstawowe funkcje, zapoznawano z bazą danych (kartotekami, słownikami). Szkolenie miało charakter prelekcji dotyczącej aplikacji, dokonano prezentacji multimedialnej (powerpoint). Podczas szkolenia uczestnicy posiadali stanowiska z dostępem do aplikacji e-Posterunek, na których wykonywano czynności w sposób praktyczny. Osoby wyznaczone do udziału w szkoleniu zobligowane były przeprowadzić analogiczne szkolenie w swoich jednostkach, a także zademonstrować sposób działania aplikacji w sposób praktyczny na komputerach posiadających już zainstalowaną aplikację. Szkolenie to odbywało się w sposób dowolny tzn. nie wyznaczono jednego konkretnego dnia na szkolenie tylko zapoznawano policjantów z e-Posterunkiem w zależności od tego kto danego dnia był w pracy zgodnie z grafikiem służb. Dlatego też wszyscy pracujący ówcześnie w WK KMP Szczecin policjanci zostali zapoznani z e-Posterunkiem w przeciągu około jednego tygodnia. Z tego też powodu szkolenie to nie zostało odnotowane w dzienniku szkoleń. Ten sam system obowiązywał w Wydziale do Walki z Przestępczością Gospodarczą KMP w Szczecinie.

(dowód: akta kontroli str.213-214)

Komendant wyjaśnił, że docelowymi użytkownikami, aplikacji e-Posterunek są wszyscy policjanci pionu dochodzeniowo-śledczego w Komendzie i nadzorowanych Komisariatach. Liczba tych osób jest zależna od stanów etatowych i na 17.12.2012 r. wynosi ok. 180. Zgodnie z założeniami użytkownikami mieli zostać również przełożeni nadzorujący pracę dochodzeniowo-śledczą oraz funkcjonariusze WRD, gdyż od kwietnia 2012 r. dostępny jest moduł tej aplikacji przeznaczony dla ruchu drogowego. Łącznie docelowymi użytkownikami aplikacji e-Posterunek powinno być ok. 200 osób. Nie została sporządzona lista osób uprawnionych do korzystania z tej aplikacji.

(dowód: akta kontroli str.330, 333-334)

Udokumentowane szkolenie w zakresie obsługi aplikacji (21.09.2010 r., 4 godziny) odbył funkcjonariusz z WK, który do końca września 2010 r. miał przeszkolić 8 funkcjonariuszy z WK. Funkcjonariusz z PG odbył 21.09.2010 r. sześciogodzinne szkolenie w zakresie aplikacji, a następnie przeprowadził 13.10.2010 r. godzinne szkolenie dla 8 funkcjonariuszy PG.

(dowód: akta kontroli str.213-214, 92)

Ustalone nieprawidłowości

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

Uwagi dotyczące badanej działalności

Ustalono, że wg stanu na 31.12.2012 r. żaden funkcjonariusz z RŁiI[28] oraz żaden z funkcjonariuszy WRD[29], nie odbył szkolenia w zakresie korzystania z aplikacji e-Posterunek.

(dowód: akta kontroli str.92, 54-62)

Szkolenia w zakresie aplikacji e-Posterunek dla funkcjonariuszy PG i WK odbyły się we wrześniu i październiku 2010 r., tj. ponad pół roku przed rozpoczęciem instalowania tej aplikacji, na sprzęcie dedykowanym, tj. maj 2011 r. (1 jednostka w WK), wrzesień 2011 r. (2 jednostki w PG, 1 w WK) i grudzień 2011 r. (po 3 jednostki w PG i w WK). Nie odbyły się szkolenia w trakcie instalowania lub po zainstalowaniu tego programu. Tylko 2 z 10 funkcjonariuszy[30], którzy użytkowali

[28] Do którego przekazano 1 notebook z zainstalowaną aplikacją e-Posterunek.

[29] Dysponujący 13 mobilnymi terminalami przewoźnymi z zainstalowaną aplikacją e-Posterunek, zamontowanymi w samochodach służbowych.

[30] WK – 5 funkcjonariuszy, PG – 5 funkcjonariuszy

sprzęt z zainstalowaną aplikacją e-Posterunek (objęty oględzinami), odbyło szkolenie z zakresu tej aplikacji (szkolenie odbyło się we IX i X 2010 r.).

(dowód: akta kontroli str.92, 54-62, 64-72)

Komendant wyjaśnił, że w żadnym szkoleniu w zakresie aplikacji e-Posterunek nie uwzględniono funkcjonariuszy RŁiI, gdyż uczestniczą oni w zapewnieniu wsparcia technicznego, a nie są odbiorcami tego narzędzia. Szkolenia z zakresu obsługi aplikacji e-Posterunek zostały zainicjowane przez KWP w 2010 r. i zostały połączone z jej instalowaniem na dostępnym wówczas sprzęcie. Szkolenia nie były powtarzane przy kolejnych dostawach sprzętu dedykowanego do e-Posterunku. Z nieustalonych przyczyn nie były podejmowane szkolenia w tym zakresie na szczeblu KMP i podległych Komisariatów. Instalacja aplikacji e-Posterunek na terminalach mobilnych nastąpiła w okresie od 26.09 do 15.10.2012 r. na polecenie Zastępcy Naczelnika WŁiI KWP. W dniu 9.01.2012 r. został zakończony proces testów odbiorczych narzędzia e-Posterunek w obszarze ruchu drogowego. KWP przekazała do KMP informację, że w lutym 2012 r. przewidziano szkolenia dla trenerów, natomiast do końca stycznia 2012 r. KMP miała otrzymać zakres i harmonogram tego szkolenia. Do 10.12.2012 r. szkolenia nie zostały przeprowadzone, nie zostały udostępnione także zakres i harmonogram szkolenia.

(dowód: akta kontroli str.97, 99, 121-127)

Wyjaśniając czy KMP w ramach sprawowanego nadzoru dysponuje informacjami: a) ilu funkcjonariuszy z nadzorowanych Komisariatów, którzy odbyli szkolenie w zakresie programu e-Posterunek, pracowało później na sprzęcie, na którym został ten program zainstalowany oraz b) ilu funkcjonariuszy z nadzorowanych Komisariatów pracuje na sprzęcie, na którym został zainstalowany program e-Posterunek bez odbycia jakiegokolwiek udokumentowanego szkolenia w jego zakresie, Komendant stwierdził, że KMP nie dysponuje takimi danymi, a ze względu na upływ czasu, fluktuację kadr oraz fakt, iż aplikacja ta w zasadzie nie jest używana zebranie takich danych może być utrudnione lub wręcz niemożliwe.

(dowód: akta kontroli str.97-98, 100)

Ocena cząstkowa

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

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

2.1. SWD.

Opis stanu faktycznego

SWD, jako podstawowa forma dokumentowania przebiegu służby, rejestru interwencji, zarządzania siłami i środkami będącymi w dyspozycji Komendy został wdrożony 21.11.2011 r. na podstawie decyzji Komendanta z 24.11.2011 r.[31], wydanej na podstawie decyzji Komendanta Głównego Policji z 27.04.2011 r. i decyzji Komendanta Wojewódzkiego Policji w Szczecinie z 21.11.2011 r. w sprawie wprowadzenia do użytku w jednostkach organizacyjnych Policji województwa zachodniopomorskiego centralnej aplikacji SWD.

(dowód: akta kontroli str.101-103)

W toku oględzin stanowiska służby dyżurnego znajdującego się w Sztabie Policji Komendy, w zakresie funkcjonowania SWD ustalono, że:

- w systemie ewidencjonowano informacje o zgłoszeniach przyjmowanych przez dyżurnych, w tym o zdarzeniach i interwencjach oraz dane dotyczące dyslokacji

[31] Nr 122/2011.

służby patrolowej, zarządzania patrolami, protokołów z odpraw do służb patrolowych;
- do systemu nie były na dzień przeprowadzenia oględzin wprowadzone grafiki służby funkcjonariuszy. Do SWD były wprowadzone grafiki służb WRD za I-XI 2012 r.;
- 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;
- wg stanu na dzień 5 grudnia 2012 r. w SWD nie była aktywna zakładka *mapa*;
- zakładki *Zarządzanie akcjami i operacjami* oraz *Zarządzanie blokadami* były aktywne, jednak nie były wykorzystywane z powodu braku takiej konieczności;
- wg stanu na dzień 11 grudnia 2012 r. była możliwość wygenerowania z systemu wszystkich raportów, poza raportem blokad SWD-R-006[32], dostępnych w zakładce kreator raportów;
- zakładka *Bieżące komunikaty* była wykorzystywana;
- istniała możliwość wygenerowania raportu odprawy zawierającego *Protokół z odprawy do służby patrolowej* na dany dzień;
- nie działały interfejsy do Wojewódzkich Centrów Powiadamiania Ratunkowego;
- nie było zakładki e-Posterunek, ani żadnego innego odesłania do aplikacji e-Posterunek;
- do kwalifikacji zdarzeń służyła zamknięta lista zdarzeń w słowniku zdarzeń. Program nie umożliwia wpisania przez dyżurnego innej klasyfikacji niż w słowniku. W dodatkowym opisie do zdarzenia użytkownik może podać uszczegółowienie zdarzenia. Słownik nie zawierał m.in. takich opisów jak: „bez uwag”[33], „rozbiegli się na widok radiowozu”, „zakłócanie ciszy nocnej”[34];
- zapis w zakładce „szczegóły zdarzenia” mógł być dokonany szarą czcionką na różowym (łososiowym) tle, co powodowało jego bardzo słabą widoczność. Zakładka służyła dyżurnym do uszczegółowienia opisu zgłaszanego zdarzenia (poza zakres jaki dopuszczał słownik). Narzędzie administratora „zarządzanie kolorami” było nieaktywne;
- dyżurny nie miał możliwości zarejestrowania zdarzenia bez podania numeru posesji;
- patrol za pomocą krótkofalówki nawiązywał kontakt z dyżurnym i ustnie informował go, np. o dotarciu na miejsce zdarzenia. Dopóki ten kontakt nie nastąpił status patrolu nie ulegał zmianie. Nie było możliwości automatycznej zmiany statusu, np. poprzez wysłanie przez patrol za pomocą krótkofalówki kodu czynności wykonywanej przez patrol, który system SWD odczytałby i automatycznie zmienił status patrolu bez potrzeby dokonania tego ręcznie przez dyżurnego;
- SWD nie był zintegrowany z system telefonów alarmowych 997 i 112. Z tego powodu w systemie nie było możliwości automatycznego wpisania w zgłoszeniu numeru telefonu zgłaszającego. Dyżury musiał ręcznie wpisać wyświetlający się numer telefonu do zgłoszenia w systemie SWD. Numer telefonu zgłaszającego był wyświetlany na małym wyświetlaczu telefonu. Operator przed odebraniem połączenia musiał spisać numeru telefonu osoby zgłaszającej, gdyż po odebraniu rozmowy, na wyświetlaczu wyświetlał się numer kolejnego abonenta usiłującego nawiązać połączenie alarmowe[35];

---

[32] Aby wygenerować raport należało podać nazwę blokady. KMP na dzień przeprowadzenia oględzin nie posiadała zdefiniowanej blokady. Tym samym tego raportu (jako jedynego) nie można było wygenerować w SWD.

[33] Np. w przypadku badania alkoholu we krwi bez jakichkolwiek innych działań.

[34] W przypadku potrzeby wpisania powodu zdarzenia.

[35] W KMP był wykorzystywany program po poprzednim systemie wsparcia dowodzenia GEMC3, aplikacja o nazwie KLIENT, która po odebraniu telefonu przez dyżurnego na stałe wyświetla numer osoby zgłaszającej (do chwili odebrania następnego połączenia).

- obraz był mało czytelny ze względu na liczbę kolumn i wierszy, jaka była zamieszczona na ekranie. SWD wyświetlał informację na dwóch ekranach. System uniemożliwiał użytkownikowi zmianę wielkości liter oraz wysokości wiersza.

(dowód: akta kontroli str.359-364, 365-457)

Rejestr interwencji Policji MS-RTJ poz. 49/11 prowadzony od 01.11.2011 r. był wykorzystywany w przypadku awarii SWD. W rejestrze w okresie od 21.11.2011 r. do 05.12.2012 r. odnotowano 28 przerw w pracy SWD, w tym jedna przerwa planowana, tj. 24.04.2012 r. od godz. 04.40 do 12.10, podczas której zaewidencjonowano 78 zgłoszeń.

(dowód: akta kontroli str.359-360)

Komendant wyjaśnił, że KMP nie prowadziła analiz związanych z awariami SWD, który jest systemem centralnym. Policjanci i pracownicy KMP są użytkownikami końcowymi tego systemu i *mogą nie posiadać wystarczającej wiedzy z zakresu funkcjonowania samego SWD jak i infrastruktury sieciowej.* Wszystkie osoby użytkujące SWD były przeszkolone z zakresu jego obsługi, ale nikt nie brał udziału w szkoleniu z zakresu usuwania awarii lub też możliwych przyczyn ich powstawania. Odnotowane przerwy w działaniu SWD w większości przypadków były niezapowiedziane i wystąpiły nagle. Tylko kilka przerw w działaniu SWD było zapowiedzianych w formie komunikatu widocznego w trakcie jego uruchamiania.

(dowód: akta kontroli str.473-474)

WP i WRD wprowadzały do SWD dane o patrolach: ich rodzaj, skład, kryptonim, rejon pełnienia służby. W WP w formie papierowej była prowadzona: Książka odpraw i wyników służby patrolowej; Książka służby w patrolach; Plan dyslokacji patroli. Powyższe książki były wykorzystywane do planowania i dyslokacji patroli. Po ich zatwierdzeniu, jakiekolwiek zmiany dotyczące patrolu mogły zostać wprowadzone za zgodą dyżurnego.

(dowód: akta kontroli str.554-555, 556-557)

W dniu 11.12.2012 r. o godz. 15.15 przystąpiono do generowania raportu SWD-R-026, w celu uzyskania informacji o ilości interwencji i czasie reakcji od pełnego wdrożenia systemu SWD, tj. od 21.11.2011 r. do 04.12.2012 r. do godz. 23.59. Raport został wygenerowany o godz. 17.16, tj. po upływie 2 godzin. W raporcie wykazano 60.955 interwencji podlegających raportowaniu; średni czas reakcji 0:24:26; mediana czasu 0:17:30; 90-ty percentyl czasu 0:51:44. Ponadto w raporcie wykazano m.in.: ilość wszystkich interwencji – 117.015; ilość interwencji własnych – 17.789; ilość zdarzeń bez udziału sił i środków – 38.265; ilość zdarzeń w trybie autonomicznym – 6.

Średni czas reakcji za I półrocze 2012 r. (29.116 interwencji) wynosił 0:26:10; mediana czasu 0:19:20; 90-ty percentyl czasu 0:54:13. Średni czas reakcji za I półrocze 2011 r. (39.831 interwencji) wynosił 0:23:40 (średnia arytmetyczna)

(dowód: akta kontroli str.364, 453-457)

Komendant wyjaśnił, że kierownictwo Komendy wykorzystuje SWD do zarządzania siłami i środkami poprzez nadzór nad zdarzeniami zarejestrowanymi w SWD, analizę zapisów książki przebiegu służby. Komendant sprawuje bezpośredni nadzór nad miernikiem „czas reakcji Policji na otrzymane zgłoszenie" określonym przez Komendanta Głównego Policji[36]. Nadzór ten odbywa się m.in. w formie

[36] W toku oględzin na podstawie raportu „Dziennik wykonań raportów SWD-R-001", ustalono, że w dniach 03-04.12.2012 r. zostało wykonanych 129 raportów, z tego: 1 raport „Historia patrolu/grupy z wyszczególnieniem rodzaju pełnionej służby SWD-R-008"; 38 raportów „Raport historii działania SWD-R-009"; 1 raport „Zestawienie ilości zdarzeń w poszczególnych kategoriach SWD-R-018"; 38 raportów „Rejestr interwencji policji SWD-R-19; 12 raportów „Rejestr zgłoszeń SWD-R-023"; 39 „Uproszczonych raportów czasów reakcji SWD-R-026".

opracowywania (w trybie codziennym, miesięcznym, kwartalnym oraz rocznym) i przedkładania Komendantowi raportów z osiągniętego czasu reakcji. Na ich podstawie są opracowywane algorytmy i sposoby postępowania, zarówno dla policjantów służb dyżurnych; policjantów służby patrolowej, którzy są kierowani do obsługi zgłoszeń, a także dla policjantów zajmujących się procesową stroną obsługi zdarzenia. Celem tych działań jest zmniejszenie aktualnie osiągniętej wartości miernika do wartości oczekiwanej przez KGP.

(dowód: akta kontroli str.470, 472, 473, 481, 368-387)

Z przeprowadzonych w Komendzie anonimowych ankiet 22 użytkowników końcowych aplikacji SWD wynika, że:
- 82% (18) oceniło, że wprowadzenie aplikacji SWD nie przyczyniło się do usprawnienia pracy i podniesienia wydajności (14%, tj. 3 ankietowanych oceniło, iż wdrożenie SWD usprawniło pracę i podniosło wydajność, 1 nie wyraził opinii);
- 96% (21) wskazało, że wdrożenie SWD nie spowodowało zmniejszenia ilości sporządzanej dokumentacji w formie papierowej (1 nie wyraził opinii);
- 59% (13) ankietowanych oceniło, iż ilość i jakość sprzętu komputerowego nie jest wystarczająca do obsługi SWD, 32% (7) oceniło, że ilość i jakość sprzętu komputerowego jest wystarczająca, 2 nie wyraziło opinii);
- 50% (11) oceniło SWD jako zły system, 41% (9) jako system średni, a 2 ankietowanych nie wyraziło opinii.

(dowód: akta kontroli str.128-171)

W ankietach, funkcjonariusze Komendy korzystający z SWD wskazywali w szczególności na następujące problemy związane z funkcjonowaniem tej aplikacji:
- mała wydajność i stabilność oraz częste zawieszanie się aplikacji;
- brak mapy miasta,
- brak przyporządkowania do ulicy odpowiedniego sektora,
- brak automatycznego wyświetlania i rejestracji numeru telefonu osoby dzwoniącej,
- brak możliwości automatycznego oddzwonienia do osoby zgłaszającej (trzeba wybierać numer ręcznie),
- mała czcionka, słaba przejrzystość,
- w zakończeniu danej interwencji brak podstawowych - często używanych formułek - kategorii wyboru, np. „nikt nie otworzył drzwi",
- brak możliwości automatycznego połączenia z patrolem za pomocą SWD, np. poprzez „kliknięcie" symbolu patrolu na ekranie komputera,
- zmiana statusu patrolu tylko drogą radiową,
- zdecydowanie sprawniejszy i przydatniejszy w pracy był poprzedni system wspomagania dowodzenia, funkcjonujący od 2001 r. GEMC3.

(dowód: akta kontroli str.128-171)

W sporządzonym w toku oględzin za 03-04.12.2012 r. raporcie SDW-R-012 „Raport o czynnościach" za dni 03-04.12.2012 r. nie zostały wykazane żadne czynności. W raporcie SWD-R-003 „Informacja o pozostających w dyspozycji siłach i środkach" sporządzonym w toku oględzin, za okres 03-04.12.2012 r. wykazywano 15.687 patroli (nawet z 2011 r., np. patrol o kryptonimie DS 870-10; status „"zaplanowany", data i godzina zmiany „2011.11.15, godz. 12:09:31"[37]). Natomiast w raporcie SWD-R-018 „Zestawienie ilości zdarzeń w poszczególnych kategoriach", wykazano 383 zdarzenia. W raporcie SWD-R-026 „Uproszczony raport czasów reakcji na zdarzenia" sporządzonym za 03-04.12.2012 r. wykazano 303 interwencje podlegające raportowaniu[38]. W raporcie analitycznym „Zestawienie zdarzeń SWD-

[37] Cały raport za dwa dni liczy 680 stron i 15687 wierszy.
[38] Średni czas reakcji: 0:15:11; mediana czasu: 0:12:20; 90-ty Percentyl czasu: 0:29:10.

RA-001" sporządzonym za 03-04.12.2012 r. zostały zaewidencjonowane 484 zdarzenia.

(dowód: akta kontroli str. 409-410, 433-436, 447-448, 451-452)

Komendant w złożonym wyjaśnieniu stwierdził, że wszystkie raporty zostały opracowane na poziomie centralnym, jako użytkownik końcowy nie ma możliwości wyjaśnienia przyczyn powyższych rozbieżności, raport SWD-R-12 nigdy wcześniej nie był generowany, a wynik raportu SWD-R-003 budzi wątpliwości, gdyż zgodnie z nazwą raportu wygenerowana liczba patroli powinna pozostawać w służbie w ciągu dwóch dni.

(dowód: akta kontroli str. 583, 586, 589-590)

Ustalone nieprawidłowości

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

Uwagi dotyczące badanej działalności

Do SWD nie były wprowadzane grafiki służb funkcjonariuszy KMP (poza WRD w okresie I-XI 2012 r.), pomimo dostępnej funkcji. NIK zwraca uwagę, że SWD jest podstawowym narzędziem dokumentowania realizacji zadań oraz odzwierciedlenia odnotowanych zdarzeń i podjętych działań.

Komendant wyjaśnił, że nie ma prawnego obowiązku prowadzenia grafiku w SWD. Brak grafiku w żaden sposób nie zmniejsza funkcjonalności SWD. Policjanci służby dyżurnej (w szczególności dyspozytorzy Pogotowia Policji) pełniący służbę na Stanowisku Kierowania nie potrzebują do właściwego zarządzania siłami i środkami grafiku policjantów. *Policjanci ci potrzebują jedynie właściwie skonfigurowanych w SWD patroli, którą to czynności wykonują kierownicy komórek organizacyjnych KMP/KP.*

(dowód: akta kontroli str.361, 556)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność kontrolowanej jednostki w przedstawionym wyżej zakresie.

2.2. e-Posterunek.

Opis stanu faktycznego

Wdrożenie w Komedzie aplikacji e-Posterunek wynikało z dyspozycji zawartych w piśmie Zastępcy Komendanta Wojewódzkiego Policji w Szczecinie z 13.09.2011 r., w którym m.in. stwierdzono: „…Dla usprawnienia wdrażania programu, już teraz proszę o spowodowanie instalacji aplikacji w komputerach użytkowanych przez policjantów prowadzących postępowania przygotowawcze. Kwestię instalacji aplikacji nadzoruje Wydział Łączności i Informatyki KWP… Zdaję sobie sprawę, że będący obecnie na stanach sprzęt jest niewystarczający zarówno ilościowo jak i technicznie do zaspokojenia pełnych potrzeb. Nie mniej mając na uwadze wyznaczony przez KGP termin wprowadzenia aplikacji, rozpoczęcie prac musi nastąpić na bazie posiadanego sprzętu…".

(dowód: akta kontroli str.213, 217-219)

Łącznie w Komendzie w latach 2010-2012 (do 31.10.2012 r.) przeprowadzono 421 postępowań przygotowawczych[39]. Żadnego postępowania nie przeprowadzono przy użyciu aplikacji e-Posterunek.

(dowód: akta kontroli str.331-332)

W wyniku oględzin sposobu funkcjonowania e-Posterunku i wykorzystania tej aplikacji przez użytkowników końcowych[40] oraz na podstawie udzielonych wyjaśnień ustalono, że:

[39] Referat Dochodzeniowo-Śledczy WK przeprowadził w 2010 r. 73 postępowania przygotowawcze, w 2011 r. 80 postępowań, a w 2012 r. (do 31.10.2012 r.) 63 postępowania. W Referacie Dochodzeniowo-Śledczym PG przeprowadzono w latach 2010-2012 odpowiednio 88, 76 i 41 postepowań przygotowawczych.

- żaden z 10 funkcjonariuszy Komendy[41] objętych badaniem nie prowadził żadnego postępowania przygotowawczego z wykorzystaniem aplikacji e-Posterunek.
- 15 funkcjonariuszy[42] nie było w stanie zalogować się do aplikacji, gdyż nie pamiętali loginu i hasła i nigdy nie korzystali z aplikacji,
- w aplikacji e-Posterunek nie było możliwości zaimportowania dokumentów zewnętrznych dotyczących prowadzonego postepowania przygotowawczego, sporządzonego przez inne niż KMP podmioty[43] (np. w formacie pdf lub doc),
- w aplikacji e-Posterunek nie było możliwości weryfikacji niepowtarzalności numeru sprawy ujmowanego w rejestrze Spraw Dochodzeniowo-Śledczych (RDS) oraz funkcji jego automatycznego nadawania, co powodowało ryzyko przypisania tego samego numeru do różnych spraw;
- w aplikacji funkcjonuje moduł zapewniający funkcję dyktafonu umożliwiającą bezpośredni zapis nagrania na nośniku wskazanym przed uruchomieniem nagrywania. Przeprowadzony w toku oględzin test polegający na nagraniu rozmowy na nośniku zewnętrznym Pendrive zakończył się niepowodzeniem,
- wg stanu na dzień 21.12.2012 r. nie działały (na zainstalowanej w Komendzie wersji 1.8.5.0 aplikacji) funkcjonalności e-Posterunku dotyczące: a) połączenia z e-PUAP[44] (użytkownik nigdy nie korzystał z tego modułu), b) połączenia z SWD oraz z KSIP (wg oświadczenia użytkownika sprawdzeń w innych centralnych policyjnych bazach danych odbywa się poza aplikacją e-Posterunek); c) zapewnienia funkcjonalności polegającej na edycji treści – bezpośrednio przed wydrukiem – tworzonych w e-Posterunku dokumentów. Możliwie było tylko dokonanie modyfikacji szaty graficznej przed wydrukiem (np. zmiana czcionki).

(dowód: akta kontroli str.485-550)

Z udzielonych przez użytkowników aplikacji wyjaśnień wynika, iż nie korzystali oni z e-Posterunku, bowiem nigdy nie otrzymali wyraźnego polecenia prowadzenia czynności służbowych przy zastosowaniu tej aplikacji lub nie wiedzieli do czego ona służy. Funkcjonariusze z PG i WK wyjaśniali, iż dysponują własną bazą szablonów dokumentów. Ponadto użytkownicy nie pamiętali lub jednoznacznie stwierdzali, że nie zostali przeszkoleni z działania e-Posterunku. Użytkownicy e-Posterunku zainstalowanego na mobilnych terminalach przewoźnych podnosili, że w przypadku wyłączenia silnika samochodu i ponownego uruchomienia system komputerowy się resetuje – wyświetlane dane są tracone.

(dowód: akta kontroli str. 485-550)

Otrzymany na potrzeby e-Posterunku sprzęt wykorzystywany był w głównej mierze do generowania dokumentów na potrzeby prowadzonych postępowań, funkcjonariusze dysponowali bazą druków procesowych w programie OpenOffice, korzystali z dostępu do aplikacji CEL, KSIP, Osadzonych i innych.

(dowód: akta kontroli str.485-550)

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

- 75% (15) oceniło, że wprowadzenie aplikacji nie przyczyniło się do usprawnienia pracy i podniesienia wydajności (5 ankietowanych nie wyraziło opinii);

---

[40] W oględzinach uczestniczyło 17 z 18 funkcjonariuszy Komendy, którym przekazano sprzęt komputerowy z zainstalowaną aplikacją e-Posterunek, tj. 5 z PG i 5 z WK (wszyscy, którzy otrzymali aplikację) oraz 7 funkcjonariuszy WRD (dowódców patroli samochodowych). KMP wskazała, że z 13 zainstalowanych mobilnych terminali przewoźnych w samochodach WRD sprawnych było 11. Przeprowadzono oględziny komputerów i aplikacji oraz testy umiejętności użytkowników w zakresie wytworzenia z wykorzystaniem e-Posterunku podstawowych dokumentów postępowania przygotowawczego. Oględzinom poddano łącznie 17 szt. sprzętu, w toku oględzin 1 mobilnego terminalu przewoźnego nie można było uruchomić.

[41] 5 z WK i 5 z PG (WRD nie prowadził postępowań przygotowawczych).

[42] 6 (1 terminal w toku oględzin był niesprawny) z WRD, 4 z WK i 5 z PG. 1 funkcjonariusz z WK zalogował się do aplikacji.

[43] Np. postanowień prokuratora o wszczęciu śledztwa, o przedstawieniu zarzutów.

[44] Elektroniczna Platforma Usług Administracji Publicznej.

- 65% (13) ankietowanych wskazało, że wdrożenie e-Posterunku nie spowodowało zmniejszenia ilości sporządzanej dokumentacji w formie papierowej (7 nie wyraziło opinii);
- 40% (8) ankietowanych oceniło, że ilość i jakość sprzętu komputerowego w Komendzie nie jest wystarczająca do obsługi e-Posterunku, 30% (6) oceniło, że jest, a 30% (6) nie wyraziło opinii;
- 10% (2) ankietowanych oceniło e-Posterunek jako system średni, 20% (4) jako zły, a 70% (14) nie wyraziło opinii.

(dowód: akta kontroli str. 172-212)

W ankietach funkcjonariusze KMP, korzystający z e-Posterunku, wskazywali w szczególności na następujące problemy związane z funkcjonowaniem tej aplikacji:
- brak możliwości automatycznego wpisywania danych podejrzanego po wprowadzeniu numeru PESEL,
- aplikacja jest przydatna jedynie w prostych postępowaniach, których przedmiotem jest jeden, dwa czyny,
- skomplikowana obsługa programu i związana z tym czasochłonność,
- nieaktualne podstawy prawne we wzorach dokumentów.

(dowód: akta kontroli str. 172-212)

WRD nie prowadził do końca 2012 żadnego postępowania przygotowawczego z zastosowaniem aplikacji e-Posterunek zainstalowanej na mobilnym terminalu przewoźnym. Komendant wyjaśnił, że instalacja aplikacji e-Posterunek w mobilnych terminalach przewoźnych miała służyć *tylko i wyłącznie* do obsługi zdarzeń drogowych, *a nie prowadzenia całych postępowań. Prowadzenie postępowań w całości w radiowozach na mobilnych terminalach przewoźnych jest niemożliwie.*

(dowód: akta kontroli str. 472, 479-480, 579)

Mobilne terminale przewoźne, na których zainstalowano aplikację e-Posterunek były na trwałe zamontowane w samochodach służbowych i nie mogły być przenoszone i wykorzystywane na miejscu zdarzenia.

(dowód: akta kontroli str. 570)

Komendant wyjaśniając czy, a jeżeli tak to w jaki sposób, aplikacja e-Posterunek, zainstalowana na mobilnych terminalach przewoźnych była wykorzystywana przez Wydział Ruchu Drogowego w listopadzie i grudniu 2012 r. stwierdził, że aplikacja nie została wykorzystana do obsługi zdarzeń drogowych, z powodu braku drukarek w radiowozach, które umożliwiałyby sporządzenie dokumentacji papierowej.

(dowód: akta kontroli str. 583, 586, 591, 595)

Na jednym urządzeniu, na którym użytkownik umiał się zalogować zainstalowana była wersja 1.8.5.0 aplikacji e-Posterunek.

(dowód: akta kontroli str. 502)

Dwa mobilne urządzenie Twinhead Durabook U12C wyposażone były w kartę SIM umożliwiającą zdalne połączenie z siecią PSTD. Z przeprowadzonych oględzin sprzętu oraz udzielonych wyjaśnień wynika, że funkcjonariusze nie używali tych urządzeń w terenie i nie dokonywali na nich sprawdzeń (np. w KSIP) poza siedzibą Komendy.

(dowód: akta kontroli str. 570, 502-507)

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 aplikacjach SWD i e-Posterunek.

3.1. SWD.

Opis stanu faktycznego

Wraz z SWD, Komenda otrzymała opracowane na szczeblu KGP dwa dokumenty dotyczące zabezpieczenia danych osobowych przetwarzanych w SWD, tj.: Polityka bezpieczeństwa SWD oraz Instrukcja zarządzania SWD.

(dowód: akta kontroli str. 16-17)

W decyzji nr 122/2011 z 24.11.2011 r. Komendant wyznaczył Naczelnika SzP na lokalnego administratora merytorycznego SWD; Kierownika RŁiI na lokalnego administratora technicznego SWD; Administratora Bezpieczeństwa Informacji KMP na Administratora Bezpieczeństwa Informacji SWD.

(dowód: akta kontroli str. 13-15)

Zgodnie z postanowieniami zawartymi w Polityce bezpieczeństwa SWD i Instrukcji zarządzania SWD, Administrator lokalny SWD w KMP prowadził wykaz pomieszczeń, w których przetwarzane są dane osobowe - *Charakterystyka Obszaru Przetwarzania Danych Osobowych* opracowaną na potrzeby SWD, *Ewidencję Udzielonych Upoważnień/Odwołań Zbioru Informacji „System Wspomagania Dowodzenia"* oraz listę osób zapoznanych z ww. dokumentami.

(dowód: akta kontroli str. 19-21, 38-45)

Z ustaleń kontroli wynika, iż każda ze 129 osób upoważnionych w Komendzie do dostępu do SWD została zapoznana z Polityką bezpieczeństwa SWD i Instrukcją zarządzania SWD.

(dowód: akta kontroli str. 38-45, 46)

Przy korzystaniu z SWD stosowane były mechanizmy kontroli dostępu do przetwarzania danych w postaci kart chipowych i haseł. Większość sprzętu komputerowego na którym zainstalowano SWD posiadało aktualne oprogramowanie antywirusowe zabezpieczające urządzenia komputerowe przed szkodliwym oprogramowaniem, które aktualizowane było automatycznie. Urządzenia komputerowe wykorzystywane do obsługi SWD nie miały połączenia z internetem, połączone były jedynie z wewnętrzną siecią PSTD[45].

(dowód: akta kontroli str. 573-577, 551-565)

W polityce bezpieczeństwa zapisano m.in., że wszystkie stanowiska dostępowe SWD, na których przetwarzane są dane osobowe powinny być podłączone do sieci zasilającej dedykowanej lub być wyposażone w UPS.

(dowód: akta kontroli str. 16-17)

Kierownik RŁiI wyjaśnił, że każda jednostka komputerowa, na której jest zainstalowana aplikacja SWD, jest podłączona do sieci zasilającej dedykowanej, która jest wyposażona w wyłączniki różnicowo-prądowe. W obiekcie KMP nie ma centralnego zasilania gwarantowanego, a stanowiska dostępowe, na których jest zainstalowane SWD nie są podłączone do dodatkowych UPS. W przypadku komputerów umieszczonych w pomieszczeniach SzP, administratorem sieci strukturalnej jest KWP. W tym obiekcie istnieje sieć zasilająca dedykowana jak również centralny UPS.

(dowód: akta kontroli str. 469)

Ustalone nieprawidłowości

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

[45] Policyjna Sieć Transmisji Danych

1. „Charakterystyka obszaru przetwarzania danych osobowych" – zatwierdzona przez Komendanta w dniu 9.11.2011 r. – stanowiąca załącznik nr 1 do Polityki bezpieczeństwa SWD, nie zawierała w szczegółowym wykazie pomieszczeń: Referatu Łączności i Informatyki; Wydziału Kryminalnego oraz SzP, w których przetwarzane były dane osobowe. Powyższy dokument o wskazane pomieszczenia został uzupełniony w toku niniejszej kontroli. Komendant wyjaśnił, że brak powyższych pomieszczeń w wykazie był spowodowany niedopatrzeniem wynikającym z koniecznością pilnego wdrożenia SWD.

(dowód: akta kontroli str. 19-21)

2. W toku oględzin (20.12.2012 r.) sprzętu komputerowego (7 zestawów stacjonarnych, tj.: 2 RSiW; 2 WP; 2 WRD, 1 WK) na którym zainstalowano SWD stwierdzono, że w 3 przypadkach programy antywirusowe były zaktualizowane przed 19.12. 2012 r., tj. 21.08.2012 r., 27.08.2012 r. i 10.09.2012 r.[46]).

(dowód: akta kontroli str. 562-565)

W pkt 5.5. Polityki bezpieczeństwa SWD m.in. zapisano, że aktualizacja baz wirusów jest wykonywana z częstotliwością uzależnioną od producenta oprogramowania antywirusowego. Raz w roku lokalny administrator techniczny sprawdza wszystkie komputery na obecność szkodliwego oprogramowania.

(dowód: akta kontroli str. 17)

Zgodnie z pkt. III ppkt 1 załącznika do rozporządzenia 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[47], system informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

Ocena cząstkowa

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

3.2. e-Posterunek

Opis stanu faktycznego

W wyniku oględzin wykorzystania e-Posterunku przez użytkowników końcowych ustalono, że w Komendzie nie przetwarzano danych osobowych w tej aplikacji.

(dowód: akta kontroli str. 331-332, 472, 485-550)

Do Komendy nie wpłynęły dokumenty dotyczące przetwarzania danych osobowych w aplikacji e-Posterunek, o których mowa w art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[48] oraz § 3 rozporządzenia MSWiA z 29 kwietnia 2004 r., tj. polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, które powinny zostać opracowane przez Komendanta Głównego Policji jako administratora danych osobowych.

(dowód: akta kontroli str. 213-215, 583, 586, 587)

Komendant wydał 16.07.2009 r. decyzję w sprawie zabezpieczenia danych osobowych w jednostkach i komórkach organizacyjnych Komendy. Decyzja została zastąpiona decyzją nr 53/2012 z 23.03.2012 r. w sprawie zabezpieczenia danych osobowych w jednostkach i komórkach organizacyjnych Komendy. Załącznik nr 1

[46] Programy te na drugi dzień zostały zaktualizowane.
[47] Dz.U. Nr 100, poz. 1024, zwane dalej *rozporządzeniem MSWiA z 29 kwietnia 2004 r.*
[48] Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.

decyzji z 23.03.2012 r. stanowiła *Polityka bezpieczeństwa przetwarzania danych osobowych w Komendzie Miejskiej Policji w Szczecinie.*

(dowód: akta kontroli str. 22-37)

Administratorem bezpieczeństwa informacji w Komendzie od 30.12.2010 r. był st. inspektor Zespołu ds. Ochrony Informacji Niejawnych.

(dowód: akta kontroli str. 37)

W § 6 ust. 2 ww. decyzji stwierdzono, że Administrator bezpieczeństwa informacji przedstawi do akceptacji Komendantowi „Instrukcje zarządzania systemem służącym do przetwarzania danych osobowych" systemów eksploatowanych w KMP w Szczecinie".

(dowód: akta kontroli str. 23)

Komenda nie opracowała Instrukcji zarządzania systemami teleinformatycznymi służącymi do przetwarzania danych osobowych. Komendant wyjaśnił, że powyższy przepis wprowadza obowiązek opracowania Instrukcji w przypadku stworzenia w Komendzie systemu teleinformatycznego. Ponieważ wszystkie używane w Komendzie systemy teleinformatyczne są ogólnopolskimi policyjnymi systemami to obowiązek opracowania instrukcji spoczywa na administratorze danego systemu, a lokalni użytkownicy mają obowiązek stosowania się do przepisów zawartych w otrzymanej dokumentacji.

(dowód: akta kontroli str. 583, 586, 587)

W przypadku badanych 10 komputerów[49] (z 12) otrzymanych przez KMP do obsługi e-Posterunku stwierdzono, że w przypadku 9 poddanych oględzinom komputerów[50], użytkownicy zalogowali się do zainstalowanego na komputerze systemu operacyjnego za pomocą loginu użytkownika i hasła logowania. W 1 przypadku logowanie następowało po zeskanowaniu linii papilarnych.

(dowód: akta kontroli str. 485-550)

Tylko w 1 przypadku na 10 poddanych oględzinom komputerów, użytkownik potrafił zalogować się do aplikacji e-Posterunek. W pozostałych przypadkach użytkownicy nie znali loginu i hasła.

(dowód: akta kontroli str. 485-550)

Urządzenia nie były podłączone do sieci zewnętrznej, a jedynie do sieci PSTD. Logowanie do e-Posterunku wymagało od każdego użytkownika podania indywidualnego hasła dostępowego. Użytkownicy nie posiadali uprawnień do instalacji dodatkowego oprogramowania na urządzeniach informatycznych. Instalacja dodatkowego oprogramowania była możliwa jedynie z poziomu administratora. W żadnym z 11 komputerach otrzymanych na potrzeby aplikacji e-Posterunek nie były zablokowane opcje Bluetooth i Wi-Fi.

(dowód: akta kontroli str. 572-576, 485-550)

Aplikacja e-Posterunek nie posiadała możliwości wymuszania zmiany hasła co 30 – 90 dni. Administratorzy lokalni nie mieli możliwości ustawienia takich zabezpieczeń bezpośrednio w aplikacji.

(dowód: akta kontroli str. 570)

Ustalone nieprawidłowości

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

[49] 3 stacjonarne i 7 przenośnych.

[50] Komputer z zainstalowaną aplikacją e-Posterunek przydzielony funkcjonariuszowi z WRG nie był pod tym zakresem poddany oględzinom. Nie poddano oględzinom komputera z zainstalowaną aplikacją e-Posterunek przekazanego do RŁiI, który udział wsparcia technicznego, a nie był odbiorcą tego narzędzia.

1. Oględziny 11 urządzeń komputerowych (3 stacjonarne i 8 przenośnych) dedykowanych do aplikacji e-Posterunek, przeprowadzone w okresie od 13.12.2012 r. do 08.01.2013 r. wykazały, iż na urządzeniach tych zainstalowane było oprogramowanie antywirusowe Dr.Web wersja 6.0.4 i 7.0. z bazą wirusów z następujących dni: 22.11.2011 r., 29.08.2012 r., 13.12.2012 r., 30.01.2012 r., 19.12.2012 r. Natomiast oględziny 6 mobilnych terminali przewoźnych z zainstalowaną aplikacją e-Posterunek (1 nie można było uruchomić w czasie oględzin) wykazały brak oprogramowania antywirusowego.

(dowód: akta kontroli str. 572-576)

Zgodnie z pkt. III ppkt 1 załącznika do rozporządzenia MSWiA z 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.

Kierownik RŁiI wyjaśnił, że aktualizacja oprogramowania antywirusowego na stanowiskach dostępowych (zarówno z zainstalowana aplikacją e-Posterunek jak i SWD) odbywała się poprzez sieć PSTD automatycznie z serwera KGP bądź KWP. Brak aktualizacji wskazywałby na odłączenie fizyczne (np. wypięcie przewodu z gniazda sieciowego) urządzenia, a tym samym brak możliwości automatycznej aktualizacji bazy wirusów.

(dowód: akta kontroli str. 570)

2. W toku oględzin ustalono, że na 2 z 7 komputerów przenośnych[51] nie zostały zainstalowane kryptograficzne zabezpieczenia danych, co było niezgodne z pkt. IV i V załącznika do rozporządzenia MSWiA z 29 kwietnia 2004 r.

(dowód: akta kontroli str. 572-576)

Kierownik RŁiI wyjaśnił, że oprogramowanie szyfrujące zgodnie z „Zaleceniami dot. standardów technicznych, użytkowych oraz bezpieczeństwa, stosowanych w policji w zakresie informatyki i łączności" instalowane ma być tylko na urządzeniach mobilnych bez względu na zainstalowane tam oprogramowanie.

(dowód: akta kontroli str. 571)

3. W 5 na 11 komputerów poddanych oględzinom, nie było wymagane hasło do wejścia do BIOS.

(dowód: akta kontroli str. 572-576)

Pkt 9.1.3. Zaleceń dotyczących standardów technicznych, użytkowych oraz bezpieczeństwa, stosowanych w Policji, w zakresie informatyki i łączności z 29.03.2012 r. stanowił, że dostęp do ustawień BIOS`u powinien być zabezpieczony co najmniej 8 znakowym hasłem (jeżeli wersja BIOS`u uniemożliwia zastosowania 8 lub więcej znakowego hasła, na maksymalną ilość znaków na jakie pozwala BIOS). Hasła należy ustawić na wszystkich kontach dostępu do BIOS.

(dowód: akta kontroli str. 596)

Kierownik RŁiI wyjaśnił, że brak hasła w systemie BIOS wynika z faktu zużywających się baterii na płycie głównej komputera. Brak zasilania lub długotrwała przerwa w pracy stanowiska komputerowego powoduje wyzerowanie ustawień BIOS`u. Po stwierdzeniu tego faktu przez pracownika RŁiI bądź zgłoszeniu go przez użytkownika, po wymianie baterii na sprawną jednostkę ponownie zostaje skonfigurowana zgodnie z „Zaleceniami dot. standardów technicznych, użytkowych oraz bezpieczeństwa…".

(dowód: akta kontroli str. 571)

[51] tj. 1 w WK i 1 w WRD. Nie poddano oględzinom komputera przekazanego do RŁiI

4. 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 rozporządzenia MSWiA z 29 kwietnia 2004 r. Maksymalny termin zmiany hasła do systemu Windows wynosił 90 dni dla 6 urządzeń do obsługi e-Posterunku (3 urządzenia użytkowane w WK KMP i 3 Wydziale PG) oraz 42 dni dla 5 urządzeń (2 urządzenia użytkowane w WK KMP, 1 w Wydziale Ruchu Drogowego KMP, 1 w SzP oraz 2 w Wydziale PG).

(dowód: akta kontroli str. 573, 576)

W 6 przypadkach funkcjonariusze stwierdzili, że system wymusza zmianę haseł co 2, 3 miesiące, w pozostałych przypadkach nie mieli takiej wiedzy lub stwierdzili, że nie wymusza takiej zmiany.

(dowód: akta kontroli str. 487, 492, 496, 500, 507, 511, 515, 519, 523, 525)

W 5 przypadkach (z 11), konfiguracja w systemie operacyjnym minimalnej długości hasła nie wymuszała na użytkowniku zastosowania w haśle minimum 8 znaków (minimalna długość hasła 0 znaków), co nie spełniało wymogów określonych w pkt IV ppkt 2 oraz pkt VIII załącznika do rozporządzenia MSWiA z 29 kwietnia 2004 r. oraz zaleceń ws. standardów bezpieczeństwa.

(dowód: akta kontroli str. 573, 576)

Zgodnie z p. IV ppkt 2 załącznika do rozporządzenia MSWiA z 29 kwietnia 2004 r. 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.

Kierownik RŁiI wyjaśnił, że zgodnie z „Zaleceniami dot. standardów technicznych, użytkowych oraz bezpieczeństwa…" dla stanowisk dostępowych podłączonych do PSTD: a) maksymalny okres ważności hasła: 180 dni; b) minimalna długość hasła: 8 znaków; c) minimalny okres ważności: nie określono; d) wymuszanie tworzenia historii haseł: 5 pamiętanych haseł. Ponadto wyjaśnił, że powyższe rozbieżności mogą wynikać z faktu konfigurowania stanowisk przez kilku administratorów w RŁiI i mogły wystąpić nieścisłości co do wprowadzania poszczególnych zasad podczas konfiguracji systemu. Obecnie w KMP i jednostkach podległych jest prowadzony przegląd całego sprzętu informatycznego pod kątem realizacji „Zaleceń dot. standardów technicznych, użytkowych oraz bezpieczeństwa, stosowanych w policji w zakresie informatyki i łączności".

(dowód: akta kontroli str. 571)

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[52], wnosi o:

1. Podjęcie działań zmierzających do zastosowania środków organizacyjnych i technicznych w celu zabezpieczenia sprzętu komputerowego przeznaczonego do obsługi e-Posterunku zgodnie z wymogami określonymi w art. 36 ustawy o ochronie danych osobowych oraz w rozporządzeniu MSWiA z 29 kwietnia 2004 r.
2. Zapewnienie bieżącej aktualizacji oprogramowania antywirusowego.

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

3. Przeszkolenie funkcjonariuszy w zakresie obsługi aplikacji e-Posterunek w sytuacji podjęcia decyzji o prowadzeniu postępowań przygotowawczych w tej aplikacji.
4. Bieżące uaktualnianie szczegółowego wykazu pomieszczeń, w których przetwarzane były dane osobowe w SWD.
5. Bieżące aktualizowanie wersji e-Posterunku zainstalowanych na urządzeniach.

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

Kontrolerzy
Jarosław Staniszewski
doradca ekonomiczny

..... *podpis*

Radosław Kropiowski
główny specjalista

..... *podpis*

Dyrektor

..... *podpis*