



Komendant
Ośrodka Szkoleń Specjalistycznych
Straży Granicznej
im. gen. bryg. Wilhelma Orlika-Rückemanna
w Lubaniu
SO-NK.0910.1.2018

Lubań, dnia 18 10.2018 r.
Egz. nr 21

ppłk SG Joanna KOSTECKA

Naczelnik Wydziału Kadr
Ośrodka Szkoleń Specjalistycznych
Straży Granicznej
im. gen. bryg. Wilhelma Orlika – Rückemanna w Lubaniu

WYSTĄPIENIE POKONTROLNE

z kontroli na temat „Przestrzeganie zasad bezpieczeństwa teleinformatycznego w systemach i sieciach teleinformatycznych”, zrealizowanej w trybie zwykłym, ujętej w „Planie kontroli przewidzianych do realizacji przez Referat Kontroli w Kierownictwie Ośrodka Szkoleń Specjalistycznych Straży Granicznej w Lubaniu na rok 2018” pod poz. 5, nr wch. 3468/17 z dnia 5.12.2017 r.

Kontrola została przeprowadzona na podstawie Wytycznych w zakresie zasad i trybu przeprowadzania kontroli w urzędach obsługujących organy lub w jednostkach organizacyjnych podległych lub nadzorowanych przez Ministra Spraw Wewnętrznych stanowiących załącznik do Decyzji Nr 65 Ministra Spraw Wewnętrznych z dnia 31 maja 2012 r. w sprawie wprowadzenia do stosowania wytycznych w zakresie zasad i trybu przeprowadzania kontroli w urzędach obsługujących organy lub w jednostkach organizacyjnych podległych lub nadzorowanych przez Ministra Spraw Wewnętrznych¹, w związku z Decyzją Nr 139 Komendanta Głównego Straży Granicznej z dnia 30 sierpnia 2012 r. w sprawie wprowadzenia do stosowania w Straży Granicznej wytycznych w zakresie zasad i trybu przeprowadzania kontroli w urzędach obsługujących organy lub w jednostkach organizacyjnych podległych lub nadzorowanych przez Ministra Spraw Wewnętrznych².

I. Oznaczenie podmiotu kontrolowanego.

Wydział Kadr³ Ośrodka Szkoleń Specjalistycznych Straży Granicznej⁴, ul. Wojska Polskiego 2, 59-800 Lubań.

Funkcję kierownika podmiotu kontrolowanego w okresie objętym kontrolą pełniła:
ppłk SG Joanna KOSTECKA⁵.

¹ Dz. Urz. MSWiA poz. 43 z późn. zm., zwanych dalej Wytycznymi.

² Dz. Urz. KGSG poz. 47, z późn. zm., zwanej dalej Decyzją nr 139.

³ Zwany dalej WK lub Wydziałem.

⁴ Zwanego dalej OSS SG lub Ośrodkiem.

⁵ Zwana dalej Naczelnikiem.

II. Imię i nazwisko, stanowisko służbowe kontrolerów, nazwa komórki kontroli oraz nr i data upoważnienia do kontroli, z uwzględnieniem zmian w okresie prowadzenia kontroli.

kierownik zespołu:

mjr SG Beata Rejczak - starszy specjalista - koordynator Referatu Kontroli w Kierownictwie OSS SG.

Upoważnienie nr 18/2018 z dnia 20.09.2018 r., ważne do dnia 19.10.2018 r.

członek:

Upoważnienie nr 17/2018 z dnia 20.09.2018 r., ważne do dnia 19.10.2018 r.

III. Data rozpoczęcia i zakończenia czynności kontrolnych w podmiocie kontrolowanym z wymienieniem dni przerw w kontroli.

Czynności kontrolne przeprowadzono w dniach 21.09 - 5.10.2018 r., z przerwami w ich prowadzeniu w dniach 22-26.09.2018 r. oraz w dniach 29-30.09.2018 r.

IV. Przedmiot kontroli i okres objęty kontrolą.

1. Przedmiotem kontroli było:

Legalność i rzetelność przestrzegania zasad bezpieczeństwa teleinformatycznego, w tym:

- a) legalność i rzetelność w przestrzeganiu zasad bezpieczeństwa teleinformatycznego przez użytkownika infrastruktury i systemów teleinformatycznych;
- b) legalność i rzetelność realizacji nadzoru służbowego nad przestrzeganiem zasad bezpieczeństwa teleinformatycznego w komórce organizacyjnej.

2. Kontrolą objęto okres od dnia 17.08.2018 r. do dnia 20.09.2018 r.

V. Ocena skontrolowanej działalności, ze wskazaniem ustaleń, na których została oparta. Zakres, przyczyny i skutki stwierdzonych nieprawidłowości oraz wskazanie osób za nie odpowiedzialnych.

Ustalenia stanu faktycznego w kontrolowanym obszarze zostały dokonane na podstawie:

1. sprawdzenia stanowisk pracy/służby z infrastrukturą i systemami teleinformatycznymi pod kątem wybranych do kontroli kwestii;
2. analizy zgromadzonej dokumentacji;
3. sporządzenia z istotnych ustaleń notatki służbowej;
4. wyjaśnień osób z podmiotu kontrolowanego.

W czterostopniowej skali ocen przyjmuje się ocenę:

➤ **Ocena pozytywna:** zostanie sformułowana, gdy w zakresie objętym kontrolą nie stwierdzono jakichkolwiek nieprawidłowości lub uchybień albo, gdy stwierdzone uchybienia miały wyłącznie charakter formalny i nie powodowały następstw dla kontrolowanej działalności, zarówno w aspekcie finansowym, jak i wykonania zadań;

➤ **Ocena pozytywna z uchybieniami:** zostanie sformułowana, jeśli stwierdzone w toku kontroli uchybienia występowały w sposób powtarzający się, lecz miały one wyłącznie charakter formalny i nie powodowały następstw dla kontrolowanej działalności, zarówno w aspekcie finansowym jak i wykonania zadań. Dodatkowo wartość miernika nie przekroczy liczby 4;

➤ **Ocena pozytywna z nieprawidłowościami:** zostanie sformułowana wówczas, gdy stwierdzone nieprawidłowości nie przekraczały założonego dla kontroli finansowej progu istotności (ze względu na wartość, charakter lub kontekst) albo, progu istotności ustalonego na podstawie cech ilościowych i jakościowych, założonego dla kontroli wykonania zadań. Dodatkowo wartość miernika nie przekroczy liczby 8;

➤ **Ocena negatywna:** gdy stwierdzone nieprawidłowości przekraczają założony dla kontroli finansowej próg istotności (ze względu na wartość, charakter lub kontekst) albo, próg istotności ustalony na podstawie cech ilościowych i jakościowych, założony dla kontroli wykonania zadań (przekroczy liczbę 12).

Realizację zadań objętych zakresem kontroli, biorąc pod uwagę kryterium legalności i rzetelności oceniono pozytywnie.

Oceny dokonano na podstawie następujących ustaleń przeprowadzonych w toku czynności kontrolnych, biorąc pod uwagę przyjęty miernik oraz przyjętą skalę ocen.

Legalność i rzetelność w przestrzeganiu zasad bezpieczeństwa teleinformatycznego przez użytkownika infrastruktury i systemów teleinformatycznych

W celu zapewnienia właściwej eksploatacji infrastruktury teleinformatycznej oraz systemów teleinformatycznych w Ośrodku wprowadzono „Zasady bezpieczeństwa teleinformatycznego w Ośrodku Szkoleń Specjalistycznych Straży Granicznej w Lubaniu”⁶, stanowiące załącznik do decyzji nr 64 Komendanta Ośrodka Szkoleń Specjalistycznych Straży Granicznej w Lubaniu z dnia 17 sierpnia 2018 r. w sprawie wprowadzenia zasad bezpieczeństwa teleinformatycznego w Ośrodku Szkoleń Specjalistycznych Straży Granicznej w Lubaniu⁷. Za ochronę informacji przetwarzanych w systemach i sieciach teleinformatycznych Straży Granicznej oraz sposoby ich zabezpieczenia, bez względu na sposób ich przetwarzania, uzyskania i przechowywania odpowiedzialni są wszyscy funkcjonariusze i pracownicy Straży Granicznej oraz inne osoby posiadające dostęp do infrastruktury Straży Granicznej. Bezpieczeństwo informacji przetwarzanych w systemach i sieciach teleinformatycznych w OSS SG, powinno być przedmiotem szczególnej troski kierownictwa i całego stanu osobowego Ośrodka (Rozdział 1 *Zasad*). Przestrzeganie *Zasad* jest obowiązkiem wszystkich funkcjonariuszy, pracowników, słuchaczy oraz gości Ośrodka będącymi użytkownikami infrastruktury teleinformatycznej oraz systemów teleinformatycznych w Ośrodku, o czym mowa w Rozdziale 6 ust. 1 *Zasad*.

Na podstawie otrzymanego z WK OSS SG wykazu o osobach pełniących służbę/zatrudnionych w Wydziale⁸ kontrolą zostało objętych 100 % stanowisk służby/pracy, na których występuje eksploatacja infrastruktury oraz praca z systemami teleinformatycznymi. Dla każdego stanowiska służby/pracy, w związku z tym, że użytkownik mógł się powtórzyć, została wypełniona odrębna tabela, służąca sprawdzeniu wybranych

⁶ Zwane dalej *Zasadami*.

⁷ Zwanej dalej Decyzją 64.

⁸ Dowód kontroli 5 (akta kontroli 5-6) - Wydruk email – lista osób z Wydziału Kadr.

wymagań bezpieczeństwa teleinformatycznego określonego wymogami Decyzji 64. Szczegółowe ustalenia zawarto w notatce służbowej z dnia 4.10.2018 r.⁹ Kontrolą objęto łącznie 15 stanowisk komputerowych użytkowanych przez 3 pracowników i 4 funkcjonariuszy¹⁰.

W ramach czynności kontrolnych sprawdzono czy praca odbywa się z aktualną wersją oprogramowania antywirusowego. Stwierdzono, że na zbadanych stanowiskach zainstalowano zalecane oprogramowanie antywirusowe McAfee, które było na bieżąco aktualizowane. Nie stwierdzono zastosowania oprogramowania innego niż licencjonowane. Nie odnotowano sytuacji działania stanowisk komputerowych z jednoczesnym wyświetlaniem się komunikatów o nieprawidłowym lub nietypowym działaniu komputera. Na skontrolowanych stanowiskach zastosowano wystarczające zabezpieczenia fizyczne przed ujawnieniem identyfikatora użytkownika oraz kod PIN do karty PKI czy haseł dostępowych. Nie stwierdzono, aby pozostawiono ww. dane w bezpośrednim sąsiedztwie stanowisk komputerowych, w miejscach widocznych dla osób postronnych. Kontrolerzy bez zastrzeżeń ocenili przechowywanie nośników danych pod kątem pozostawiania ich bez nadzoru. Zbadane podczas czynności kontrolnych nośniki danych (IND) były zaewidencjonowane bądź w Rejestrach Wydanych Dokumentów (RWD) bądź na indywidualnej karcie użytkownika. Wygaszacz ekranu we wszystkich sprawdzonych sprzętach był zabezpieczony hasłem, a w przeglądarkach wyłączona opcja zapamiętywania haseł. Ustalono, że zastosowano właściwą konfigurację sprzętu komputerowego m.in. dokonano aktualizacji systemu operacyjnego do Windows 10 oraz użytkowano dedykowany w Straży Granicznej program antywirusowy McAfee.

Zgodnie z zapisami Rozdziału 2 ust. 1 i ust. 3 *Zasad* wszyscy funkcjonariusze i pracownicy WK OSS SG podpisali oświadczenia, których podpisanie stanowiło warunek dostępu do zasobów teleinformatycznych Ośrodka. W czynnościach kontrolnych sprawdzono zarówno jego zgodność ze wzorem jak i jego ważność. W związku z terminem wejścia w życie Decyzji 64 za aktualne uważane były oświadczenia podpisane od dnia 17.08.2018 r. Wszystkie zbadane oświadczenia spełniły ten warunek. Sporządzone i wypełnione zostały w oparciu o obowiązujący wzór. W kontroli zbadano także czy dostęp użytkowników do zasobów teleinformatycznych Ośrodka odbywał się w zakresie niezbędnym do realizacji zadań służbowych. Poprzez wyszukiwanie obecności plików o rozszerzeniu „.jpg”, „.mp3”, „.dvd”. Sprawdzone czy na mieniu ruchomym Straży Granicznej nie przechowywano i nie przetwarzano informacji prywatnych. Skontrolowano również poprzez dokonanie przeglądu historii stron internetowych czy nie korzystano z portali społecznościowych i innych, niezwiązanych z pracą na komputerach służbowych. Tylko w 1 przypadku¹¹ stwierdzono obecność 5 zdjęć o charakterze prywatnym, co stanowi uchybienie dla zapisów Rozdziału 2 ust. 4 *Zasad* (dostęp użytkowników do zasobów teleinformatycznych Ośrodka odbywa się w zakresie niezbędnym do realizacji zadań służbowych) oraz Rozdziału 3 ust. 10 lit. a) tiret 28 *Zasad* (zabrania się przechowywania i przetwarzania informacji prywatnych na mieniu ruchomym Straży Granicznej). Zgodnie z przyjętymi od Naczelnika wyjaśnieniami¹² były to zdjęcia z 2015 roku, o których przechowywaniu użytkownika komputera zapomniała. Uchybienie zostało usunięte w trakcie trwania kontroli. Za powyższe uchybienie odpowiada bezpośrednio użytkownik danego komputera, natomiast z racji sprawowanego nadzoru Zastępca Naczelnika Wydziału Kadr wykonujący jednocześnie zadania kierownika Sekcji Spraw Osobowych oraz Naczelnik. Ww. uchybienie o charakterze formalnym, nie miało żadnych skutków ani znaczącego wpływu na kontrolowaną działalność.

⁹ Dowód nr 6 (akta kontroli 7-38) – *Notatka służbowa*.

¹⁰ Stan osobowy podmiotu kontrolowanego wynosił 9 osób, w tym 2 osoby w okresie objętym kontrolą z usprawiedliwionych przyczyn służbowych nie korzystały z infrastruktury teleinformatycznej Wydziału.

¹¹ Użytkownik

¹² Dowód kontroli 8 (akta kontroli 40-41) - *Protokół przyjęcia ustnych wyjaśnień pptk SG Joanny Kosteckiej*.

Zespół kontrolny w celu sprawdzenia czy przetwarzano informacje niejawne poza miejscami specjalnie do tego wyznaczonymi dokonał sprawdzenia opracowywanych materiałów pod kątem zawierania nazw „zastrz”, „pouf” i „taj”. Nie znaleziono dokumentów o charakterze niejawnym.

W przypadku stanowisk podłączonych do sieci Internet zbadano, na podstawie losowo wybranych dokumentów, czy nie są wykonywane dokumenty zawierające dane wrażliwe. O ile takich dokumentów nie znaleziono, to kontrolerzy stwierdzili u jednego z użytkowników¹³ obecność 2 dokumentów, otrzymanych drogą elektroniczną w drodze czynności służbowych związanych ze składaniem ofert na stanowiska w Ośrodku,¹⁴ zawierających wrażliwe dane; m.in. imię, nazwisko, adres, data urodzenia, adres email, nr telefonu, stan cywilny itp.

Chociaż nie były to dokumenty, których zabrania się wykonywać użytkownikowi na stanowiskach komputerowych podłączonych do sieci Internet w rozumieniu zapisów Rozdział 3 ust. 10 lit. a) tiret 15 *Zasad* - tylko stanowiły pliki w formacie „pdf”, otrzymane od kandydatów do służby/pracy w Ośrodku, zawierały one jednak wrażliwe dane.

Mimo, iż zespół kontrolny nie uznał tego za uchybienie, gdyż zapisy Decyzji 64 mówią o dokumentach wytwarzanych przez użytkownika, to jednak w świetle otrzymanych od Naczelnika wyjaśnień¹⁵ tj., że otrzymane za pośrednictwem poczty zewnętrznej dokumenty przed wydrukiem do dalszych celów służbowych, zostają zapisane w komputerze, przechowywanie tych plików w komputerze z dostępem do Internetu, uznał za nieuzasadnione i niewłaściwe praktyki. Omawiane pliki w wersji elektronicznej zostały usunięte w trakcie czynności kontrolnych.

Zgodnie z zapisami Rozdziału 3 lit. c) tiret 1 *Zasad* do obowiązków użytkownika należy samodzielnie wykonywanie, z wykorzystaniem informatycznych nośników danych (IND), kopii zapasowych dokumentów przetwarzanych na stacjach dostępowych.

Jak wynika z ustaleń kontroli część dokumentacji, w szczególności tej wytwarzanej na komputerach z dostępem do Internetu np. wzór kwestionariusza, szablon pisma przewodniego do przesłania wniosku nie wymagała tworzenia ich kopii zapasowych i użytkownicy ich nie tworzyli lub nie stwierdzono obecności materiałów, których kopie należałoby zabezpieczyć.¹⁶ Odnosnie komputerów bez dostępu do sieci Internet, w przypadku 4 użytkowników¹⁷ w ocenie kontrolerów taki obowiązek powinien być jednak wykonywany. W związku z powyższym zapytano Naczelnika o badaną kwestię.

Wg uzyskanych wytłumaczeń¹⁸ dokumenty wytworzone przez Naczelnika są zapisywane na dysku D, lecz nie są to treści, których utrata spowodowałaby konieczność ich odtworzenia lub przechowywania na nośnikach zewnętrznych. Część dokumentacji przechowywanej przez nią w komputerze są to pisma przesłane przez podwładnych pracowników i funkcjonariuszy. Dokumenty są drukowane i przesyłane zgodnie z właściwością, a większość dokumentów wykorzystywana jest, jako szablony do tworzenia nowych pism. Wg Naczelnik istotne dane, w tym zbiory statystyczne i zestawienia są opracowywane, co do zasady przez jej Zastępcę wykonującego jednocześnie obowiązki Kierownika Sekcji Spraw Osobowych, która je gromadzi i na bieżąco uzupełnia. Odnosnie osób podległych Naczelnik wyjaśniła, że wg użytkowników dane, które są zapisane na komputerze nie wymagają sporządzania kopii zapasowych. Są to pisma bieżącego użytku, które po sporządzeniu są drukowane i przekazywane jej do podpisu lub dla Komendanta Ośrodka. Większość dokumentów wykorzystywana jest jako szablony do tworzenia nowych pism.

¹³

¹⁴ „ ” oraz „ ”

¹⁵ Dowód kontroli 8 (akta kontroli 40-41) - *Protokół przyjęcia ustnych wyjaśnień ppłk SG Joanny Kosteckiej.*

¹⁶ Dowód nr 6 (akta kontroli 7-38) - *Notatka służbowa.*

¹⁷

¹⁸ Dowód kontroli 8 (akta kontroli 40-41) - *Protokół przyjęcia ustnych wyjaśnień ppłk SG Joanny Kosteckiej.*

Otrzymane wyjaśnienia zespół kontrolny uznał za wystarczające i przyjął, że zapis Decyzji 64 dotyczy materiałów merytorycznie ocenionych, jako wymagające sporządzenia kopii zapasowej, a nie obligatoryjnie wszystkich. Potencjalnym skutkiem nie tworzenia kopii zapasowych dokumentów jest ich częściowa lub nieodwracalna utrata np. w przypadku awarii sprzętu czy też działania innych czynników, powodująca konieczność poświęcenia ponownego czasu służbowego na ich ewentualne odtworzenie. Złożone przez Naczelnik wyjaśnienia wskazują na brak takiego zagrożenia tj. konieczności odtwarzania dokumentów u wskazanych użytkowników. Jednocześnie ww. wskazała, że konieczność tworzenia kopii zapasowych dokumentów występuje na stanowisku Zastępcy Naczelnika Wydziału. W kontroli zostało potwierdzone, że takie działania na ww. stanowisku były realizowane.

Kontrolowany obszar, mimo stwierdzonego uchybienia, biorąc pod uwagę przyjęty miernik oceniono **pozytywnie**.

Legalność i rzetelność realizacji nadzoru służbowego nad przestrzegania zasad bezpieczeństwa teleinformatycznego w komórce organizacyjnej

Sprawowanie nadzoru nad przestrzeganiem i realizacją postanowień zawartych w szczególnych wymaganiach bezpieczeństwa i procedurach bezpiecznej eksploatacji systemu teleinformatycznego w Wydziale należy do obowiązków Naczelnika Wydziału, wskazanych w ust. 2 pkt. 19) załącznika nr 1 do Decyzji nr 6 Komendanta Ośrodka Szkoleń Specjalistycznych Straży Granicznej w Lubaniu z dnia 9 stycznia 2017 r. w sprawie *określenia szczegółowego zakresu obowiązków i uprawnień Naczelnika Wydziału Kadry Ośrodka Szkoleń Specjalistycznych Straży Granicznej w Lubaniu*. Odpowiednio do zapisów Rozdziału 2 ust. 3 *Zasad* Naczelnik przechowywał oświadczenia osób zatrudnionych/pośredniczących służbę w WK OSS SG, dotyczące zapoznania z „Zasadami bezpieczeństwa teleinformatycznego w OSS SG”, które były zgodne ze wzorem określonym w Decyzji 64.

Ustalenia kontroli w obszarze przestrzegania zasad bezpieczeństwa teleinformatycznego przez poszczególnych użytkowników infrastruktury i systemów teleinformatycznych u podległych funkcjonariuszy i pracowników pozwalają stwierdzić, iż Naczelnik właściwie realizował nadzór służbowy nad przestrzeganiem i realizacją postanowień zawartych w szczególnych wymaganiach bezpieczeństwa i procedurach bezpiecznej eksploatacji systemu teleinformatycznego w komórce organizacyjnej.

Kontrolowany obszar, biorąc pod uwagę kryterium legalności i rzetelności oceniono **pozytywnie**.

- VI. **Zalecenia lub wnioski dotyczące usunięcia nieprawidłowości lub usprawnienia funkcjonowania podmiotu kontrolowanego.**
W związku z tym, że kontrolowana działalność została oceniona pozytywnie nie sformułowano zaleceń i wniosków pokontrolnych.
- VII. **Zgodnie z § 34 Wytycznych, w związku z Decyzją nr 139 od wystąpienia pokontrolnego nie przysługują środki odwoławcze.**
- VIII. **Wystąpienie pokontrolne sporządzono w dwóch jednobrzmiących egzemplarzach, z których jeden przeznaczony jest dla kierownika podmiotu kontrolowanego i zostanie przekazany poprzez Kancelarię Tajną Sekcji Ochrony Informacji Wydziału Ochrony Informacji OSS SG, drugi ad acta Referat Kontroli w Kierownictwie OSS SG.**

IX. Fakt przeprowadzenia kontroli odnotowano w „Księżce kontroli OSS SG”, zarejestrowanej w Rtd nr 10/2009 pod pozycją nr 8 w 2018 roku, prowadzonej przez Referat Kontroli OSS SG.

wz. KOMENDANT
Centrum Szkoleń Specjalistycznych Straży Granicznej
im. gen. bryg. Wilhelma Orlika-Rückemanna
w Lubaniu

plk SG Małgorzata SAKALUK

18 PAŹ. 2018

.....
(stopień, imię i nazwisko, stanowisko oraz podpis
zarządzającego kontrolę)

Wykonano w 2 egzemplarzach:

Egz. nr 1 – Naczelnik Wydziału Kadr OSS SG.

Egz. nr 2 - ad acta Referat Kontroli w Kierownictwie OSS SG

Sporz./Wyk.: Rejczak (tel.6664265)

Dnia: 18.10.2018 r.