Ekonomiczne Problemy Usług nr 2/2018 (131), t. 1

ISSN: 1896-382X | www.wnus.edu.pl/epu
DOI: 10.18276/epu.2018.131/1-32 | strony: 323–330

Kamila Schneider, Karol Schneider
Uniwersytet Szczeciński
kamilaschneider@interia.pl

Zagrożenia w funkcjonowaniu jednolitego pliku kontrolnego

Kod JEL: M48
Słowa kluczowe: jednolity plik kontrolny, ewidencja VAT w formie elektronicznej, zagrożenia JPK w firmie, zzależnienia od Microsoftu
Streszczenie. Celem artykułu jest przedstawienie problemów wynikających z obowiązku przesyłania plików JPK_VAT dla małych i średnich przedsiębiorstw. Od 2016 roku prowadzone jest sukcesywne uszczelnianie systemu podatkowego. Jednym z jego elementów jest obowiązkowe raportowanie rejestrów sprzedaży i zakupu VAT. Na podstawie nowelizacji ustawy z dnia 29 sierpnia 1997 r. Ordynacja Podatkowa (Dz.U. 2015, poz. 613 ze zm.) podatnicy podatku od towarów i usług są zobowiązani do przekazywania danych z ksiąg podatkowych w formie tzw. jednolitego pliku kontrolnego (JPK). JPK jest to uniwersalny standard elektroniczny pliku, opartego na formacie xml. Plik musi zawierać oczekiwane dane podatkowe, uporządkowane ściśle według wymogów Krajowej Administracji Skarbowej, przestawionych na stronach Ministerstwa Finansów. Błędy i zaniedbania związane z raportowaniem JPK mogą prowadzić do poważnych konsekwencji karnoskarbowych jak kary porządkowe i grzywny.

Wprowadzenie

Jednolity Plik Kontrolny (*Standard Audit – File* – SAF – T; dalej: JPK) jest zbiorem danych, tworzonym z systemów informatycznych podmiotu gospodarczego poprzez bezpośredni eksport danych, zawierającym informacje o operacjach gospodarczych za dany okres, posiadającym ustandaryzowany układ i format (schemat xml) umożliwiający jego łatwe przetwarzanie. Chodzi o to, aby można było w sposób automatyczny, przy wykorzystaniu odpowiednich algorytmów informatycznych, wyodrębnić niezbędne dane merytoryczne. Intencją tych rozwiązań było wprowadzenie do systemów księgowych nowej funkcjonalności, tj. możliwości edycji ksiąg podatkowych oraz dowodów księgowych

w oparciu o powszechnie stosowany w komunikacji elektronicznej standard XML. Rozwiązanie to funkcjonowało już w wielu innych krajach Unii Europejskich (Czechy, Holandia, Portugalia, Włochy itd.) (Wszystko o…, 2016, s. 4).

Celem zmian miało być zmniejszenie kosztów wypełniania obowiązków podatkowych przez podatników i ich kontrahentów, zmniejszenie kosztów funkcjonowania administracji skarbowej oraz poprawa wyników kontroli. Od 1 stycznia 2018 roku wszystkie przedsiębiorstwa będące płatnikami podatku VAT będą przesyłać do Krajowej Administracji Skarbowej miesięczne obowiązujące dane poprzez JPK.

Również od 1 lipca 2018 roku wszyscy, którzy prowadzą księgowość w formie elektronicznej, będą musieli przekazywać inne struktury JPK na żądanie organów podatkowych. Obejmują one: księgi rachunkowe (JPK_KR), wyciągi bankowe (JPK_WB), magazyn (JPK_MAG), faktury VAT (JPK_FA), podatkową księgę przychodów i rozchodów (JPK_PKPIR) oraz ewidencję przychodów (JPK_EWP).

Status przedsiębiorcy na potrzeby wysyłki dokumentów JPK ustala się w oparciu o przepisy ustawy o swobodzie gospodarczej z dnia 2 lipca 2004 roku (Dz.U. 2016, poz. 1829).

1. Zagrożenia w systemie informatycznym przedsiębiorstwa

Jednostki gospodarcze, rozszerzając zakres komputerowo przetwarzanych, przechowywanych i przesyłanych danych, narażają się na coraz większe ryzyko spowodowane naruszeniem tajności oraz poufnych danych, a skutkami negatywnymi tych zagrożeń mogą być skutki finansowe, które wynikają z (Nowicki, 1988, s. 247):

- poszerzania dodatkowych nakładów na niezbędne zabezpieczenia,
- strat spowodowanych przerwami w funkcjonowaniu firmy,
- wzrostu opłat ubezpieczeniowych, sankcji finansowych za nierealizowanie zasad określonych w obowiązującym prawie,
- odszkodowań płaconych różnym podmiotom,
- nakładów na przywrócenie sprawności różnym składnikom systemu informacyjnego i połączeń między podsystemami.

Przestępstwa i oszustwa komputerowe, bezpieczeństwo danych i systemów komputerowych oraz zagrożeń w systemie informatycznym rachunkowości przedsiębiorstw omawia K. Schneider (2007, s. 60–85). Potrzeba zapewnienia bezpieczeństwa wzrasta proporcjonalnie do znaczenia informacji we współczesnym świecie.

Jak słusznie zauważa D.R. Pipkin (2002, s. 13), instytucje powinny wprowadzić efektywne środki bezpieczeństwa zapewniające ochronę informacji posiadanej przez firmę, ciągły dostęp do systemów podtrzymujących funkcje krytyczne oraz odpowiednie mechanizmy zabezpieczenia informacji przed jej rozmyślnym lub przypadkowym ujawnieniem, manipulacją, modyfikacją, zniszczeniem lub skopiowaniem.

W ochronie danych mogą być stosowane różne metody. Do podstawowych metod ochrony zalicza się (Kolbusz, Rejer, 2006, s. 295–303):

- organizacyjne i administracyjne,
- techniczne,
- programowe,
- szyfrowania danych,
- prawne.

Z powyższych metod szyfrowanie danych jest najbardziej skutecznym sposobem ochrony danych. Technika szyfrowania, czyli kryptografia, polega na przedstawianiu bloku danych za pomocą odpowiedniego klucza tajnego (prywatnego) lub jawnego (znanego wszystkim użytkownikom). Wyróżnia się szyfrowanie (Ferguson, Schneider, 2004, s. 35, 277):

- symetryczne – szyfrowanie i deszyfrowanie odbywa się za pomocą tego samego klucza (uważane jest za mniej przydatne w Internecie),
- asymetryczne – oparte na kluczu publicznym udostępnianym wielu użytkownikom i na kluczu prywatnym, który jest znany tylko jego właścicielowi (do szyfrowania i deszyfrowania używa się różnych kluczy).

Zagrożenia w systemie informatycznym przedsiębiorstwa można zakwalifikować według następujących kryteriów (Schneider, 2016, s. 143):

1. Ze względu na źródło mogą to być zagrożenia:
   - wewnętrzne, na które jednostka ma wpływ – wśród nich wyróżnia się zagrożenia:
   a) organizacyjne, wynikające z nieprawidłowej organizacji jednostki,
   b) technologiczne, będące następstwem błędów technologicznych,
   c) zewnętrzne, pochodzące z otoczenia jednostki gospodarczej.
2. Ze względu na celowość działań mogą to być zagrożenia:
   - przypadkowe (losowe),
   - celowe (umyślne).
3. Ze względu na rodzaj zagrożenia mogą to być zagrożenia w stosunku do:
   - oprogramowania,
   - sprzętu.
4. Ze względu na wynik zagrożenia można mówić o:
   - całkowitej utracie danych,
   - kradzieży informacji (wycieku danych),
   - ingerencji w przetwarzane dane.

Właściwie nie ma sposobu na zupełne zabezpieczenie komputerów, ale należy prowadzić działania minimalizujące zagrożenia. Problem ten jest znaczący, ponieważ ogromne zagrożenie bezpieczeństwa systemów informatycznych wynika z działalności ludzi.

2. Zagrożenia w polskiej administracji publicznej

Polska administracja publiczna jest uzależniona od Microsoftu. W podobnej sytuacji jest coraz więcej krajów, ponieważ informacje o państwach i ich obywatelach przechowywane są w wirtualnej chmurze tej firmy. Uzależnienie od informatycznego gigan-

ta nie dość, że kosztuje miliony, to jeszcze może stanowić zagrożenie dla bezpieczeństwa publicznego i obywateli. Władze nie mogą zagwarantować prywatności danych przy pracy z oprogramowaniem, którego nie kontrolują.

Wedle ostrożnych szacunków Microsoft w latach 2015 i 2016 na sektorze publicznym w Unii Europejskiej zarobił około 2 mld dolarów. W Europie na oprogramowanie firmy Microsoft trzeba wydać 200 euro rocznie dla każdego urzędnika (Cieśla, 2017). W Polsce koszt pojedynczej licencji Microsoftu jest różny, w zależności od tego, kto płaci. Szacuje się, że każdy urząd co roku wydaje na licencje Microsoftu od kilku do kilkuset milionów złotych. Na przykład MON w latach 2006–2016 wydało na ten cel 163 mln zł. ZUS w latach 2011–2015 wydał na licencje 17 mln zł, ale na serwery tej samej firmy ponad 75 mln zł. Ministerstwo Kultury na zakupione licencje na Windowsa zapłaciło 600 tys. zł, a Ministerstwo Sprawiedliwości za ponad dwa razy więcej licencji wydało wielokrotnie mniej (Cieśla, 2017). Faktem jest, że około 98% administracji publicznej jest uzależniona od Microsoftu.

W Polsce momentem uzależnienia od Microsoftu jest pojawienie się Płatnika, czyli stworzonego przez Prokom programu do przesyłania elektronicznych dokumentów ubezpieczeniowych do ZUS. Musi to robić każda firma. Program był bezpłatny, ale działa wyłącznie pod systemem Windows.

Polskie urzędy administracji samorządowej wprowadziły program o nazwie Bestia, którym raportują wykonanie budżetów izbom obrachunkowym. Program ten działa wyłącznie na licencji Microsoftu, a to oznacza, że 2,5 tys. gmin musiało kupić system Windows. Uzależnienie od programu Microsoftu wciąż w Polsce rośnie.

3. Informatyzacja służb skarbowych (JPK)

W czerwcu 2016 roku powołano spółkę celową Aplikacje Krytyczne dla informatyzacji służb skarbowych. JPK Analizator jest to narzędzie informatyczne służące do automatycznych analiz danych zawartych w plikach JPK VAT. Generuje ono automatycznie raporty, które pokazują m.in. niezgodność kwot w plikach JPK VAT i deklaracjach VAT złożonych przez podatników za ten sam okres. Wskazują też rozbieżność kwot jednej transakcji, przedstawionych przez dwóch podatników z złożonych przez nich plikach JPK (Pogroszewska, 2017).

Ministerstwo Finansów podało, że na podstawie plików JPK złożonych na luty i marzec 2017 roku zidentyfikowano około 8 tys. przypadków rozbieżności między plikami JPK VAT i deklaracjami VAT za te miesiące. Z danych informatycznych wynika, że firmy składające JPK uwzględniły za luty i marzec 2017 około 25 tys. faktur wystawionych przez podmioty, które nie posiadają statusu czynnego podatnika VAT.

W praktyce występują nieprawidłowości w funkcjonowaniu analiz JPK. Stosowane rozwiązania informatyczne są dość proste, ale często generują błędy – podatnicy otrzymują z systemu JPK błędne komunikaty, co nie świadczy najlepiej o jakości tych rozwiązań. Ale to nie znaczy, że nie należy udoskonalić Analizatora JPK (narzędzie

informatyczne). Wprowadzenie „twardej" analityki pozwoli na identyfikowanie przestępstw podatkowych, karuzel VAT itp. Wprowadzenie kompleksowych narzędzi pozwoli wykryć sieć powiązań między kontrahentami. Analizator pozwoli również dokonać analiz branżowych dotyczących obrotu poszczególnymi towarami (Jędrzejewska, 2017).

4. Wiedza przedsiębiorców dotycząca JPK

Na podstawie przeprowadzonych badań można stwierdzić, że informacje o obowiązku wprowadzenia JPK są niewystarczające, co obrazują dane zawarte w tabeli 1. Z badań z października 2017 roku, przeprowadzonych przez Instytut Badań i Rozwiązań B2B Keralla Research na próbie 500 firm techniką wywiadów telefonicznych wynika, że firmy duże i średnie nie obawiają się JPK.

Tabela 1. Ocena zmian prawnych na krajową gospodarkę

Ocena wpływu JPK	%	Uwagi
Pozytywnie	42,0	
Neutralnie	21,8	
Negatywnie	12,4	
Nie ma zdania	23,5	

Źródło: R. Skibińska (2017). *Firmy nie obawiają się JPK. Rzeczpospolita*, 22.12, *297.*

Wpływ nowego obowiązku JPK w działalności firmy według oceny przedsiębiorstw przedstawiono w tabeli 2.

Tabela 2. Wpływ JPK na działalność firmy

Ocena nowego obowiązku	%	Uwagi
Pozytywnie	10,8	
Neutralnie	59,6	
Negatywnie	16,4	
Nie ma zdania	13,2	

Źródło: R. Skibińska (2017). *Firmy nie obawiają się JPK. Rzeczpospolita*, 22.12, *297.*

Przedsiębiorcy obawiają się, że wprowadzenie JPK zwiększy i tak już liczne prace księgowości, ponieważ oprócz raportowania JPK obowiązuje również raportowanie do GUS, ZUS, organów skarbowych, NBP, banków. Oznacza to więcej pracy nad sprawozdawczością i wyższy koszt prowadzenia działalności gospodarczej.

Nowy obowiązek jest szczególnie negatywnie oceniany wśród mikroprzedsiębiorstw. Spośród badanych 1000 małych firm przez „in Fakt", wysyłki JPK organom podatkowym większość z nich oceniła negatywnie, co ukazano w tabeli 3.

Tabela 3. Ocena JPK przez mikroprzedsiębiorców

Ocena mikroprzedsiębiorców	%	Uwagi
Negatywnie	49	Idea dobra, jaka będzie praktyka?
Neutralnie	25	
Pozytywnie	15	
Idea jest dobra, ale?	7	
Muszą Się Przygotować Do Nowego Nieuchronnego Obowiązku	4	

Źródło: *Puls Biznesu* (2017). 19.12, *242*.

Z powyższej tabeli wynika, że tylko 15% respondentów pozytywnie ocenia nowy obowiązek.

W innej ankiecie odpowiedzi na pytanie, jak przygotowane są do JPK mikroprzedsiębiorstwa, przedstawiono w tabeli 4.

Tabela 4. Przygotowanie mikroprzedsiębiorców do JPK

Treść	%	Uwagi
Szykują się do nowego obowiązku	10	
Nie wie czy jego program księgowy jest przygotowany do wysyłki JPK	70	
Posiadane systemy pozwalają na wysyłki JPK	13	
Na razie nie są przygotowani, ale zapewniają, że będą na czas	13	
Nie myśli o przygotowaniu do nowego obowiązku	25	
Martwi się, że ma niewystarczającą wiedzę i może popełnić błąd	33	
Poradzą sobie dzięki pomocy biur rachunkowych	37	

Źródło: *Puls Biznesu* (2017). 19.12, *242*.

Z przeprowadzonych przez nas badań na grupie 61 studentów ekonomii na Wydziale Zarządzania i Ekonomiki Usług Uniwersytetu Szczecińskiego nikt nie wiedział, co to jest JPK – jednolity plik kontrolny.

Wśród klientów naszych biur rachunkowych na 112 ankietowanych:

- 6% wiedziało co to jest JPK – byli to przedsiębiorcy zobowiązani do wysyłania JPK od 1.01.2017,
- 13% wiedziało z prasy, że dotyczy ich obowiązek wysyłki pliku JPK od 1.01.2018 r.
- 38% dowiedziało się z listu z ZUS, w którym otrzymali numer konta, że mają obowiązek wysyłania JPK,
- 43% nie wie, co to jest JPK, po to mają biuro rachunkowe, żeby się tym nie zajmować.

Podsumowanie

Wiedza o JPK wśród przedsiębiorców, a więc przede wszystkim zainteresowanych, jest niewielka. Odpowiedzialność za wysyłkę JPK cedują na służby finansowo-księgowe lub biura rachunkowe.

Korzyści, jakie widzą przedsiębiorcy w związku z obowiązkiem dostarczania JPK:

- mniej kontroli w przedsiębiorstwie przez urzędy skarbowe, gdyż wszystkie operacje będą w comiesięcznych raportach JPK-VAT,
- przekazywanie dokumentów do urzędu skarbowego elektronicznie w plikach, nie ma potrzeby nosić ich fizycznie,
- eliminacja kontroli losowych,
- ograniczenie nieuczciwej konkurencji,
- w przyszłości wycofanie deklaracji VAT7,
- przyspieszenie zwrotu nadpłaconej kwoty VAT.

Negatywne skutki wprowadzenia obowiązku JPK:

- wzrost kosztów, niekiedy konieczność nowego sprzętu i aktualizacja oprogramowania do wysyłki JPK,
- koszty szkolenia pracowników.

Literatura

Cieśla, W. (2017). Skolonizowani przez Microsoft. *Nesweek Polska, 17* (18–23.04), 71–72.

Ferguson, N., Schneider, B. (2004). *Kryptografia w praktyce*. Gliwice: Helion.

Jędrzejowska, K. (2017). W lipcu nasza „twarda" analityka danych JPK. *Dziennik Gazeta Prawna, 126* (3.07).

Kolbusz, E., Rejer, J. (2006). *Wstęp do informatyki w zarządzaniu*. Szczecin: Wydawnictwo Naukowe Uniwersytetu Szczecińskiego.

Nowicki, A. (1988). *Informatyka dla ekonomistów. Studium teoretyczne i praktyczne*. Warszawa–Wrocław: Wydawnictwo Naukowe PWN.

Pipkin, D.L. (2002). *Bezpieczeństwo informacji. Ochrona globalnego przedsbiębiorstwa*. Warszawa: WNT.

Pogruszewska, M. ((2017). Automatyczna analiza JPK pokaże, kto oszukuje. *Rzeczpospolita*, *152* (3.07).

Schneider, K. (2016). *Patologie i oszustwa gospodarcze po transformacji ustrojowej*. Szczecin. PTE.

Wszystko o jednolitym pliku kontrolnym (2016). *Rzeczpospolita*.

HAZARDS IN THE FUNCTIONING OF THE SINGLE CONTROL FILE

Key words: Standard Audit – File – SAF – T, VAT register in electronic form, Standard Audit – File – SAF – T threat in the company, Addiction from Microsoft

Summary. Purpose – aim of this article is to present the problems arising from the obligatory to transfer files JPK_VAT for small and medium -sized enterprises.

Since 2016, gradual sealing of the tax system has been carried out. One of its elements is obligatory reporting of sales and VAT purchase registers. Standard Audit – File – SAF – T (JPK) is a universal electronic standard file, based on the xml format. The file must contain the expected tax data, arranged in strict accordance with the requirements of the National Tax Administration, presented on the website of the Ministry of Finance. Mistakes and negligence related to JPK reporting can lead to serious fiscal consequences such as fine and fine.

Translated by Kamila Schneider

Cytowanie

Schneider, K., Schneider, K.. (2018). Zagrożenia w funkcjonowaniu jednolitego pliku kontrolnego. *Ekonomiczne Problemy Usług*, *2* (131/1), 323–330. DOI: 10.18276/epu.2018.131/1-32.