STUDIA I PRACE
Kolegium Zarządzania i Finansów
ZESZYT NAUKOWY 157

157/2017
s. 69–87

Szkoła Główna Handlowa w Warszawie
Oficyna Wydawnicza SGH
kolegia.sgh.waw.pl

Jolanta Wiśniewska
Uniwersytet Mikołaja Kopernika w Toruniu

Bezpieczeństwo informacji a ryzyko przestępczości komputerowej

Streszczenie

Rozwój nowych technologii oraz globalny rynek kształtują otaczającą nas rzeczywistość. Szczególnie dynamicznie ewoluują systemy komputerowe, w tym również systemy informatyczne rachunkowości. Rachunkowość jako jeden z najważniejszych elementów systemu informacyjnego jednostki gospodarczej jest szczególnie narażona na zagrożenia wynikające z rozwoju nowoczesnych technologii komputerowych i rynku globalnego. Celem artykułu jest przedstawienie uregulowań prawnych oraz zagrożeń, wynikających z rozwoju nowych technologii, dla działalności gospodarczej, a w szczególności dla systemu informacyjnego przedsiębiorstw, metod ich wykrywania i zapobiegania. W dobie ciągłych cyberataków liczą się przede wszystkim szybkie i sprawne działania w celu zapobiegania takim zagrożeniom, synchronizujące technologię, działania prawne i zarządzanie komunikacją. Cyberbezpieczeństwo przy tak dynamicznym rozwoju nowoczesnych technologii stało się strategiczną koniecznością.

Słowa kluczowe: rachunkowość, przestępczość komputerowa, rachunkowość śledcza, cyberbezpieczeństwo
Kody klasyfikacji JEL: M41, M48

1. Wprowadzenie

Według EY rozwój nowych technologii oraz globalnego rynku należą do sześciu globalnych megatrendów[1] kształtujących otaczającą nas rzeczywistość[2]. W szczególności szybkim rozwojem charakteryzują się zintegrowane systemy komputerowe typu ERP. Intensywny rozwój technologii informatycznych dotyczy również systemów informatycznych rachunkowości. Rachunkowość jest ważnym elementem systemu informacyjnego jednostki gospodarczej. Jest ona we współczesnym rozumieniu systemem informacyjnym, którego celem jest pomoc interesariuszom w procesie podejmowania decyzji gospodarczych, finansowych, jak również jest narzędziem, który ma za zadanie rozliczanie kierownictwa z zarządzania powierzonym mu mieniem[3]. Zatem jest ona w szczególności narażona na zagrożenia wynikające z rozwoju nowoczesnych technologii komputerowych i rynku globalnego. Według badań przeprowadzonych przez PwC liczba wykrytych incydentów naruszających bezpieczeństwo informacji w 2015 r. wzrosła na świecie w stosunku do roku poprzedniego o 38%, natomiast w Polsce aż o 46%[4].

Celem artykułu jest przedstawienie uregulowań prawnych oraz zagrożeń dla rachunkowości, wynikających z rozwoju nowych technologii, metod ich wykrywania i zapobiegania.

Do realizacji sformułowanego celu zastosowano następujące metody badawcze: studium literatury przedmiotu, analizę aktów prawnych regulujących zagadnienia dotyczące przestępstw komputerowych i cyberbezpieczeństwa, studium wyników badań dotyczących występowania cyberataków w Polsce i na świecie oraz metodę analizy przypadków dotyczących usług z zakresu cyberbezpieczeństwa organizacji.

---

[1] Megatrendy stanowią połączone globalne siły, mające wpływ na wszystkich ludzi poprzez zmianę społeczeństwa, kultury oraz gospodarki. Pozwalają na lepsze zrozumienie zarówno wyzwań, jak i szans stojących przed współczesnym biznesem, EY, *Megatrends 2015. Making Sense of a Word in Motion*, http://www.ey.com, dostęp 09.11.2016, s. 2; patrz także: PwC, *W obronie cyfrowych granic czyli 5 rad, aby realnie wzmocnić ochronę firmy przed CYBER ryzykiem*, Warszawa, https://www.pwc.pl, dostęp 10.11.2016, s. 4.

[2] EY, *Megatrends...*, op.cit., s. 2; patrz także: KPMG, *Future State 2030: Światowe wyzwania dla liderów i przywódców*, https://www.kpmg.com/PL/pl, dostęp 2.11.2016, s. 1–3; PwC, *W obronie...*, op.cit., s. 4.

[3] B. Kunz, A. Tymińska, *System informatyczny rachunkowości i jego rola w świetle ustawy o rachunkowości*, „Nauki o Finansach" 2014, nr 3(20), s. 44.

[4] PwC, *W obronie...*, op.cit., s. 4.

2. Rachunkowość jako system informacyjny przedsiębiorstw

Rachunkowość jako „międzynarodowy język biznesu"[5] była wielokrotnie definiowana. W tabeli 1 zostały przedstawione wybrane definicje pojęcia „rachunkowość".

Tabela 1. Wybrane definicje pojęcia „rachunkowość"

Autor	Definicja pojęcia „rachunkowość"
W. Brzezin	System informacyjny organizacji gospodarczych o charakterze retro- i prospektywnym, który posiada własny algorytm rachunku ekonomicznego i metody ustalenia, planowania oraz analizy wyniku finansowego w pewnym okresie oraz kondycji finansowej w ściśle określonym momencie czasowym
E. Burzymowa	Uniwersalny, podmiotowy system informacyjno-kontrolny
S. Skrzywan	Ogół metod i zabiegów rachunkowych, systematycznych i dorywczych, stosowanych w przedsiębiorstwie celem stworzenia podstaw dla decyzji kierowniczych
A. Jarugowa	Pomiar oraz analiza relacji i interakcji związanych z przenoszeniem i tworzeniem, podziałem i ewentualnie utratą wartości, zarówno jako nośników użyteczności (wartości użytkowej), jak i mierników wartości. Współcześnie jest ona postrzegana jako prawnie regulowany, specyficzny system informacyjny, tworzący liczbową reprezentację sytuacji finansowej i wyników działalności podmiotu gospodarczego
S. Sojak	Pewien system identyfikacji, pomiaru, przetwarzania i przekazywania informacji finansowych o sytuacji majątkowej i osiąganych wynikach – służący celom sprawozdawczym i decyzyjnym różnych podmiotów (użytkowników)

Źródło: opracowanie własne na podstawie: W. Brzezin, *Rachunkowość sensu stricto i sensu largo*, „Zeszyty Teoretyczne Rachunkowości" 2000, t. 56, s. 18; E. Burzym, *Rachunkowość przedsiębiorstwa i instytucji*, PWE, Warszawa 1980, s. 13; S. Skrzywan, *Rachunkowość w przedsiębiorstwie przy gospodarce planowej. Cele i funkcje*, Prace Zakładu Rachunkowości SGH w Warszawie, nr 1, Gospodarczy Instytut Wydawniczy, Warszawa 1948, s. 11; A. Jarugowa, *Niektóre wyznaczniki rozwoju rachunkowości*, w: *Współczesne problemy rachunkowości*, red. A. Jarugowa, PWE, Warszawa 1991, s. 13; A. Jarugowa, *Wprowadzenie – istota zmian w ustawie o rachunkowości i ich skutki ekonomiczne*, w: *Komentarz do ustawy o rachunkowości. Rachunkowość – MSR – Podatki*, red. A. Jarugowa, T. Martyniuk, Ośrodek Doradztwa i Doskonalenia Kadr, Gdańsk 2002, s. 51; S. Sojak, *Pojęcie rachunkowości*, w: *Podstawy rachunkowości*, red. S. Sojak, J. Stankiewicz, TNOiK, Toruń 2008, s. 21.

Cechą wspólną wszystkich przedstawionych definicji pojęcia „rachunkowość" jest to, że stanowi ona system informacyjny, będący podstawą podejmowania decyzji. To jeden z najważniejszych elementów systemu informacyjnego przedsiębiorstwa,

[5] E.A. Hendriksen, M.F. van Breda, *Teoria rachunkowości*, Wydawnictwo Naukowe PWN, Warszawa 2002, s. 35; W. Brzezin, *Ogólna teoria rachunkowości*, Wyższa Szkoła Handlu i Prawa, Warszawa 1998, s. 22; E. Walińska, *Międzynarodowe Standardy Rachunkowości*, Oficyna Ekonomiczna, Kraków 2006, s. 15; J. Turyna, *Rachunkowość finansowa*, C.H. Beck, Warszawa 2005, s. 9–16.

ewoluuje wraz z jego rozwojem. Na globalnym konkurencyjnym rynku informacja w różnych przekrojach informacyjnych o charakterze zarówno retro- jak i prospektywnym[6] stała się nie tylko koniecznością, lecz także towarem, nie zawsze pozyskiwanym w sposób legalny.

Najbardziej efektywnym i najważniejszym narzędziem, który stanowi podstawę systemu informacyjnego rachunkowości, jest system informatyczny[7]. Wraz z rozwojem technologii również systemy informatyczne ewoluowały od prostych systemów finansowo-księgowych do systemów ERP.

W Polsce zasady prowadzenia ksiąg rachunkowych i sporządzania sprawozdań finansowych reguluje ustawa o rachunkowości[8]. Zgodnie z art. 10 ust. 1 ustawy, każda jednostka powinna posiadać dokumentację opisującą przyjęte przez nią zasady (politykę) rachunkowości, w tym zasady dotyczące prowadzenia ksiąg rachunkowych przy użyciu komputera. Ponadto dokumentacja ta powinna zawierać wykaz zbiorów danych, tworzących księgi rachunkowe na informatycznych nośnikach danych z określeniem ich struktury, wzajemnych powiązań oraz ich funkcji w organizacji całości ksiąg rachunkowych i w procesach przetwarzania danych, z opisem systemu informatycznego zawierającego wykaz programów, procedur lub funkcji, w zależności od struktury oprogramowania, wraz z wyjaśnieniem algorytmów i parametrów. Jednostki mają obowiązek zawarcia w polityce rachunkowości informacji dotyczącej wersji oprogramowania i daty rozpoczęcia jego eksploatacji. Ustawa reguluje także obowiązki w zakresie cech ksiąg rachunkowych prowadzonych z użyciem komputera, obowiązkowe elementy dotyczące zapisów księgowych i wydruków komputerowych oraz warunki uznania zapisów na trwałych nośnikach danych. Ważny element dokumentacji opisującej zasady prowadzenia ksiąg rachunkowych stanowi opis programowych zasad ochrony danych, w tym w szczególności metod zabezpieczenia dostępu do danych i systemu ich przetwarzania[9].

Rozwój technologii spowodował, że 57% informacji jest generowana wyłącznie w formie elektronicznej, a 43% w formie papierowej[10], co wymusza na organizacjach

[6] W. Brzezin, *Ogólna*..., op.cit., s. 18.

[7] Por. A. Jabłoński, M. Kawczyńska, Ż. Pietrzak, T. Wnuk-Pel, *Oczekiwany wpływ implementacji zintegrowanego systemu informatycznego na jakość informacji – studium przypadku*, „Zeszyty Teoretyczne Rachunkowości" 2016, t. 89(145), s. 57; B. Kunz, A. Tymińska, *System*..., op.cit., s. 44–45.

[8] Ustawa z dnia 29 września 1994 r. o rachunkowości, Dz.U. z 2016 r., poz. 1047 ze zm.

[9] Ibidem, art. 10, 13, 14.

[10] J. Góra, *Raport. Efektywne zarządzanie bezpieczeństwem informacji*, Ślązak, Zapiór i Wspólnicy, Media Recowery, https://www.us.edu.pl, dostęp 08.11.2016, s. 4.

stosowanie coraz bardziej zaawansowanych technologicznie zabezpieczeń. Uregulowania zawarte w ustawie o rachunkowości mają za zadanie systemowe zapewnienie bezpieczeństwa prowadzeniu ksiąg rachunkowych za pomocą komputera i ochronę danych, co przy aktualnej dynamice rozwoju technologicznego i globalizacji staje się priorytetem w walce z przestępczością komputerową.

3. Przestępczość komputerowa

Rozwój technologii komputerowych ma wpływ na współczesne życie i gospodarkę zarówno w skali mikro, jak i makro[11]. Ma on również wpływ na działalność przedsiębiorstw, kształtuje ich rozwój, a to z kolei na coraz większe zapotrzebowanie na wszelkiego rodzaju informacje. Z drugiej jednak strony, rozwój nowych technologii, do których można zaliczyć m.in. Internet, urządzenia mobilne, media społecznościowe, chmury obliczeniowe, duże zbiory danych (ang. *big data*), sprzyja powstawaniu coraz nowszych rodzajów przestępstw z ich udziałem bez ograniczeń terytorialnych[12]. Można zatem stwierdzić, że działalność gospodarcza prowadzona jest obecnie w erze cyberataków i kryzysu zaufania[13].

Opracowanie i wdrożenie właściwych aktów prawnych stanowi główny środek w przeciwdziałaniu rosnącym przypadkom cyberprzestępczości[14]. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW określa rodzaje zagrożeń dotyczących przestępczości komputerowej. Wykaz zagadnień, określanych mianem ataków na systemy informatyczne, przedstawiono w tabeli 2.

[11] Por. N. Kshetri, *Positive Externality, Increasing Returns, and the Rise in Cybercrimes*, „Communications of the ACM" 2009, vol. 52, no. 12, s. 141–144.

[12] Por. EY, *Megatrends...*, op.cit., s. 4; patrz także: N. Kshetri, *Positive...*, op.cit., s. 141–144.

[13] Por. PwC, *W obronie...*, s. 1.

[14] C. Barclay, *Using Frugal Innovations to Support Cybercrime Legislations in Small Developing States: Introducing the Cyber-Legislation Development and Implementation Process Model (CyberLeg-DPM)*, „Information Technology for Development" 2014, vol. 20, no. 2, 165–195; patrz także: K.L. Hui, S.H. Kim, Q.H. Wang, *Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks*, „MIS Quarterly" 2017, vol. 41, no. 2, s. 497–523.

Tabela 2. Cyberprzestępstwa – prawo unijne

Rodzaj przestępstwa komputerowego	Art.	Charakterystyka
Niezgodny z prawem dostęp do systemów informatycznych	3	Umyślne i bezprawne uzyskiwanie dostępu do całości lub jakiejkolwiek części systemu informatycznego
Niezgodna z prawem ingerencja w systemy	4	Umyślne i bezprawne poważne utrudnienie lub zakłócenie funkcjonowania systemu informatycznego poprzez wprowadzenie, przekazywanie, uszkadzanie, usuwanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych lub czynienie ich niedostępnymi
Niezgodna z prawem ingerencja w dane	5	Umyślne i bezprawne usuwanie, uszkadzanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych w systemie informatycznym lub czynienie ich niedostępnymi
Niezgodne z prawem przechwytywanie danych	6	Umyślne i bezprawne przechwytywanie środkami technicznymi niepublicznych przekazów danych komputerowych do, z lub w ramach systemu informatycznego, w tym emisji elektromagnetycznych z systemu informatycznego zawierającego takie dane komputerowe

Źródło: opracowanie własne na podstawie: Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW, Dz.U. UE L 218 z dnia 14.08.2013 r.

Ogólne zagadnienia opisujące rodzaje przestępstw komputerowych określa prawo unijne, natomiast poszczególne kraje ustanawiają przepisy szczegółowe. Wybrane uregulowania prawne dotyczące przestępstw komputerowych w Polsce przedstawiono w tabeli 3.

Tabela 3. Cyberprzestępstwa – prawo polskie

Akt prawny	Przepis	Charakterystyka
Kodeks karny Rozdział XXXIII Przestępstwa przeciwko ochronie informacji	Art. 265	Nieuprawnione wykorzystanie informacji niejawnych o klauzuli „tajne" lub „ściśle tajne"
	Art. 266	Nieuprawnione ujawnianie lub wykorzystanie informacji w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową
	Art. 267	Uzyskanie dostępu do informacji przeznaczonych dla innych osób, polegające na otwieraniu zamkniętego pisma, podłączaniu się do sieci telekomunikacyjnej lub przełamywaniu albo omijaniu elektronicznych, magnetycznych, informatycznych lub innych szczególnych zabezpieczeń
	Art. 268	Niszczenie, uszkadzanie, usuwanie lub zmiana zapisów istotnej informacji albo w inny sposób udaremnianie lub znaczne utrudnianie osobie uprawnionej zapoznania się z nią

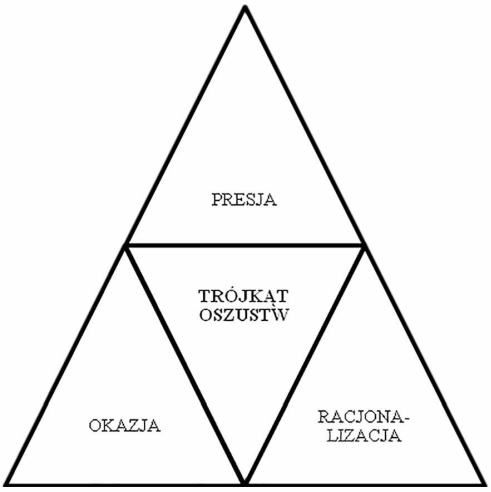
Akt prawny	Przepis	Charakterystyka
Kodeks karny Rozdział XXXIII Przestępstwa przeciwko ochronie informacji	Art. 268a	Niszczenie, uszkadzanie, usuwanie, zmiana lub utrudnianie dostępu do danych informatycznych albo w istotnym stopniu zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych
	Art. 269	Niszczenie, uszkadzanie, usuwanie lub zmiana danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych. Niszczenie poprzez wymianę informatycznych nośników danych lub przez uszkodzenie urządzeń służących do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych
	Art. 269a	Przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej
	Art. 269b	Wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie innym osobom urządzenia lub programu komputerowego przystosowanego do popełnienia przestępstwa, a także hasła komputerowego, kodu dostępu lub innych danych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej
Ustawa o zwalczaniu nieuczciwej konkurencji	Art. 23	Ujawnianie innej osobie lub wykorzystanie we własnej działalności gospodarczej informacji stanowiących tajemnicę przedsiębiorstwa uzyskanych w związku z pełnioną funkcją lub uzyskanych bezprawnie
Ustawa o ochronie danych osobowych	Art. 49	Przetwarzanie danych osobowych w zbiorze bez prawa przetwarzania tych danych
	Art. 52	Przy administrowaniu danymi naruszanie choćby nieumyślnie obowiązku zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem
	Art. 53	Niezgłaszanie do rejestracji zbioru danych przez osoby obowiązane

Źródło: opracowanie własne na podstawie: Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, Dz.U. z 1997 r. nr 88 poz. 533 ze zm.; Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, Dz.U. z 2003 r. nr 153, poz. 1503 ze zm.; Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. z 2015 r., poz. 2135 ze zm.

Według D.R. Cresseya oszustwa dotyczące działalności gospodarczej, a szczególnie systemu informacyjnego organizacji, opierają się na tzw. trójkącie oszustw[15], który został przedstawiony na rysunku 1.

[15] J.T. Wells, *Nadużycia w firmach. Vademecum. Zapobieganie i wykrywanie*, LexisNexis, Warszawa 2006, s. 6–15.

Rysunek 1. Trójkąt oszustw



Źródło: opracowanie własne na podstawie: J.T. Wells, *Nadużycia w firmach. Vademecum. Zapobieganie i wykrywanie*, LexisNexis, Warszawa 2006, s. 7.

Trójkąt oszustw ma również zastosowanie do cyberataków. Ryzyko jest tym większe, im więcej występuje słabych stron w organizacji systemu informacyjnego przedsiębiorstwa, co stwarza okazje dla przestępców. W badaniach przeprowadzonych przez EY[16] respondenci dokonali oceny słabych stron organizacji systemu informacyjnego, mających wpływ na zwiększenie ryzyka cyberataków. Ocena 1 oznaczała największe ryzyko, a ocena 5 najmniejsze (tabela 4).

Z badań przedstawionych w tabeli 4 wynika, że największym zagrożeniem dla powstawania cyberataków w pierwszej kolejności jest czynnik ludzki, czyli niestaranni i nieświadomi pracownicy, których działania lub brak działań w największym stopniu wpływają na wzrost ryzyka powstawania przestępstw komputerowych. W następnej kolejności największa liczba respondentów wskazała na brak aktualnych kontroli bezpieczeństwa informacji lub jej architektury. Z analizy czynników

[16] Badanie EY było skierowane do dyrektorów ochrony informacji, dyrektorów finansowych, prezesów i innych menedżerów zajmujących się ochroną informacji. Zostało przeprowadzone w okresie od czerwca do września 2015 r. W badaniu wzięło udział 1755 respondentów z 67 krajów, reprezentujących 25 głównych gałęzi przemysłu, którzy otrzymali kwestionariusz ankietowy. Większość odpowiedzi zebrano podczas wywiadów „face to face". Gdy nie było to możliwe, kwestionariusz został wypełniony przez Internet, EY, *Creating trust in the digital world. EY's Global Information Security Survey 2015*, http://www.ey.com, dostęp 9.11.2016, s. 30–31.

o największym ryzyku należy stwierdzić, iż są to czynniki wynikające z wewnętrznej struktury organizacji systemu informacyjnego, a dopiero na końcu z racji korzystania z mediów publicznych. Potwierdza to ocena respondentów dotycząca najmniejszego ryzyka, gdzie największa liczba respondentów wskazała na użytkowanie publicznych mediów społecznościowych i korzystanie z publicznej (niezabezpieczonej) chmury obliczeniowej (po 23%). Przy analizie tabeli 4 narzuca się wniosek, że pomimo wzrastającego zagrożenia przestępczością komputerową, największa liczba ocen dotycząca czynników stanowiących słabe punkty organizacji została oceniona na poziomie średniego ryzyka (ocena 3).

Tabela 4. Słabe strony organizacji systemu informacyjnego przedsiębiorstw (w %)

Ocena / Słabe punkty	1	2	3	4	5
Użytkowanie publicznych mediów społecznościowych*	6	14	31	25	23
Korzystanie z publicznej (niezabezpieczonej) chmury obliczeniowej	10	18	28	21	23
Korzystanie z mobilnych aplikacji komputerowych	9	23	31	22	15
Nieaktualne kontrole bezpieczeństwa informacji lub jej architektury	15	19	31	19	16
Nieautoryzowany dostęp	10	22	36	20	12
Niestaranni lub nieświadomi pracownicy*	18	26	32	14	9

* Dane z badania nie sumują się do 100%.

Źródło: opracowanie własne na podstawie: EY, *Creating Trust in the Digital World. EY's Global Information Security Survey 2015*, http://www.ey.com, dostęp 9.11.2016, s. 6.

Ważnym zagadnieniem dotyczącym wykrywalności cyberataków jest identyfikacja ich sprawców. Badania przeprowadzone przez PwC[17] wskazały główne źródła ataków, co zostało zaprezentowane w tabeli 5.

W tabeli 5 przedstawiono strukturę sprawców przestępstw komputerowych w Polsce na tle świata – zarówno w Polsce, jak i na świecie głównymi sprawcami cyberataków byli pracownicy. Również inne wyniki badań oraz literatura przedmiotu potwierdzają wiodącą rolę pracowników wśród sprawców cyberataków[18]. Natomiast

[17] W badaniu przeprowadzonym przez PwC wzięło udział 126 polskich ekspertów zajmujących się IT i bezpieczeństwem informacji. Zostało one przeprowadzone jesienią 2015 r. metodą ankiety *online*, PwC, *W obronie...*, op.cit., s. 23.

[18] Por. J. Mayer, *Cybercrime Litigation*, „University of Pennsylvania Law Review" 2016, vol. 164, s. 1502; KPMG, *Profil korporacyjnego oszusta*, https://assets.kpmg.com, dostęp 15.11.2016, s. 21; J. Góra, *Raport...*, op.cit., s. 11–12; EY, *Creating...*, op.cit., s. 12.

jeżeli chodzi o pozostałe grupy cyberprzestępców, to ich struktura kształtowała się odmiennie. W Polsce w drugiej kolejności sprawcą cyberataków byli nieznani hakerzy, następnie przestępcy z grup zorganizowanych i ostatnią główną grupą byli obecni dostawcy i wykonawcy. Odmiennie kształtowała się struktura sprawców przestępstw komputerowych na świecie: w drugiej kolejności odnotowano incydenty z udziałem byłych pracowników, a następnie obecnych dostawców i wykonawców.

Tabela 5. Główni sprawcy cyberataków w 2015 r. (w %)

Wyszczególnienie	Polska	Świat
Pracownicy	70	34
Byli pracownicy	–	29
Nieznani hakerzy	67	–
Przestępcy z grupy zorganizowanej	41	–
Obecni dostawcy i wykonawcy	35	19

Źródło: opracowanie własne na podstawie: PwC, *W obronie cyfrowych granic, czyli 5 rad, aby realnie wzmocnić ochronę firmy przed CYBER ryzykiem*, https://www.pwc.pl, dostęp 10.11.2016, s. 10.

W wyniku cyberataków jednostka ponosi wiele konsekwencji, które mają na nią wpływ zarówno w krótkim, jak i dłuższym okresie. Do konsekwencji tych należą m.in. nadszarpnięcie reputacji i marki jednostki, poniesienie przez jednostkę odpowiedzialności cywilnej, wystąpienie zagrożeń dla działalności przedsiębiorstwa, powstanie szkód finansowych, naruszenie interesów klientów/kontrahentów czy też ukaranie osób odpowiedzialnych za bezpieczeństwo informacji w firmach[19]. Konsekwencje cyberprzestępczości w polskich firmach przedstawiono w tabeli 6.

Tabela 6. Konsekwencje cyberataków w polskich firmach w 2015 r.

Wyszczególnienie	Udział w %
Utrata klientów	33
Straty finansowe	33
Ujawnianie lub modyfikacja danych	31
Utrata reputacji	16

Źródło: jak pod tab. 5, s. 8.

[19] Por. J. Góra, *Raport...*, op.cit., s. 9.

Z wyników badań przedstawionych w tabeli 6 wynika, że w polskich firmach skutkami cyberataków są prawie w takim samym stopniu utrata klientów, straty finansowe oraz ujawnianie lub modyfikacja danych.

4. Działania dotyczące cyberbezpieczeństwa w firmach

W dobie ciągłych cyberataków liczy się przede wszystkim szybka i sprawna reakcja na incydenty. Taka, która synchronizuje technologię, działania prawne i zarządzanie komunikacją[20]. Ponad 77% organizacji zdaje sobie sprawę z wartości posiadanych przez nich informacji, a to z kolei ma wpływ na coraz większą świadomość potrzeby działań prewencyjnych[21]. Według badań przeprowadzonych przez KPMG w 2015 r. 29% prezesów firm wymienia cyberbezpieczeństwo jako problem, który ma obecnie największy wpływ na funkcjonowanie firm[22].

Bardzo ważne dla bezpieczeństwa informacji jest zrozumienie wyzwań z tym związanych. Według EY w celu skutecznego rozpoznania i odpowiedniej reakcji na niebezpieczeństwa związane z cyberprzestępczością, organizacje muszą posiadać odpowiednią wiedzę i zrozumieć ich istotę. Każda jednostka powinna posiadać informacje na temat aktualnych rodzajów cyberataków, w jaki sposób te ataki są przeprowadzane, jak jest do tego przygotowana i jak można temu przeciwdziałać[23].

W badaniach przeprowadzonych przez EY respondenci dokonali oceny ryzyka występowania zagrożeń dotyczących systemu informacyjnego organizacji; ocena 1 oznaczała największe ryzyko, a ocena 5 najmniejsze (tabela 7).

Największe zagrożenie, zdaniem respondentów (19%) stanowi ryzyko wyłudzania informacji, na drugim miejscu znalazły się zagrożenia dotyczące złośliwego oprogramowania i ataków typu „godzina-zero" (po 16%), a na trzecim wskazane zostały ryzyko cyberataków dotyczących kradzieży informacji finansowych i zakłócających

[20] PwC, *W obronie...*, op.cit., s. 1.

[21] J. Góra, *Raport...*, op.cit., s. 4.

[22] Dane oparte zostały na badaniu ankietowym przeprowadzonym wśród 1276 prezesów firm z Australii, Chin, Francji, Niemiec, Indii, Włoch, Japonii, Hiszpanii, Wielkiej Brytanii i USA. Respondenci reprezentowali dziewięć kluczowych branż: motoryzację, bankowość, ubezpieczenia, zarządzanie inwestycjami, opiekę zdrowotną, technologię, handel detaliczny / rynki konsumenckie, energetykę oraz usługi komunalne; KPMG, *Cyberbezpieczeństwo – wyzwanie współczesnego prezesa*, https://assets.kpmg.com, dostęp 8.11.2016, s. 4.

[23] EY, *Creating...*, op.cit., s. 2; patrz także Deloitte, *Beneath the Surface of a Cyberattack. A Deeper Look at Business Impacts*, https://www².deloitte.com, dostęp 15.11.2016, s. 2.

pracę organizacji lub niszczących organizację (po 15%). Zdaniem respondentów najmniejsze zagrożenie dla systemu informacyjnego organizacji stanowią klęski żywiołowe (35%). Natomiast najmniejsze ryzyko cyberataków dotyczy kradzieży informacji finansowych. Takie wskazanie respondentów może mieć swoje uzasadnienie wymogami prawnymi, które ich zdaniem, wymuszają na jednostkach opracowanie i wdrożenie procedur bezpieczeństwa informacji.

Tabela 7. Zagrożenia systemu informacyjnego organizacji (w %)

Zagrożenia \ Ocena	1	2	3	4	5
Klęski żywiołowe (huragany, powodzie itp.)	9	11	23	22	35
Szpiegostwo (np. przez konkurencję)	9	14	24	22	31
Cyberataki dotyczące kradzieży własności intelektualnej lub danych	13	17	26	22	21
Ataki wewnętrzne (np. przez niezadowolonych pracowników)	9	18	32	23	19
Cyberataki dotyczące kradzieży informacji finansowych	15	18	25	19	23
Cyberataki zakłócające pracę organizacji lub niszczące organizację	15	18	29	19	19
Oszustwa	12	22	28	19	19
Spamy	9	19	36	22	13
Ataki typu „godzina-zero"	16	19	32	16	17
Wyłudzanie informacji	19	25	29	16	12
Złośliwe (szkodliwe) oprogramowanie (np. wirusy, robaki i konie trojańskie)	16	27	30	18	9

Źródło: jak pod tab. 4, s. 6.

Po dokonaniu analizy ryzyka poszczególnych zagrożeń dotyczących cyberataków, organizacja powinna przystąpić do działań mających za zadanie przeciwdziałanie/obronę przed tego typu incydentami. Wdrożenie systemu zarządzania ryzykiem jest istotnym elementem bezpieczństwa informacji. EY zidentyfikowało trzy fundamentalne bloki budowania cyberbezpieczeństwa (tabela 8).

Pomimo świadomości i wdrażania w przedsiębiorstwach rozwiązań dotyczących cyberbezpieczeństwa informacji, skuteczność działania stosowanych rozwiązań bardzo często jest niewystarczająca. Badania przeprowadzone przez EY wskazały na ograniczenia mające wpływ na skuteczność ochrony informacji (tabela 9).

Tabela 8. Fundamenty budowania cyberbezpieczeństwa w firmie

Podstawowe fundamenty cyberbezpieczeństwa	Charakterystyka
Przewidywanie (ang. *anticipate*)	Organizacje powinny budować solidne fundamenty cyberbezpieczeństwa, które powinny obejmować kompleksowy zestaw środków bezpieczeństwa informacji, będących podstawą obrony przed cyberatakami. Na tym etapie organizacje ustalają podstawy cyberbezpieczeństwa w firmie
Dostosowanie się (ang. *adapt*)	Organizacje w celu przetrwania na konkurencyjnym rynku powinny dostosowywać się do zmieniających się warunków. W związku ze zmianami w działalności gospodarczej również zagrożenia ulegają ewolucji, dlatego podstawą środków bezpieczeństwa informacji powinno być nadążanie za zmianami, ponieważ inaczej z upływem czasu staną się coraz mniej skuteczne. Na tym etapie jednostki powinny dostosować organizację cyberbezpieczeństwa do zmieniających się wymagań
Aktywacja (ang. *activate*)	Organizacje muszą opracować taktykę wykrywania i zmniejszenia ryzyka potencjalnych cyberataków. Muszą określić swoje potrzeby dotyczące ochrony swoich najcenniejszych aktywów i opracować scenariusze odpowiedzi na prawdopodobne zagrożenia cybernetyczne, co wymaga od nich zdolności wywiadowczych, opracowania metodologii oceny ryzyka, odpowiednich mechanizmów reagowania na incydenty i odpowiedniej organizacji. Na tym etapie jednostki określają swoją zdolność do obrony przed cyberzagrożeniami i niespodziewanymi atakami, jak również przewidują tego typu incydenty

Źródło: opracowanie własne na podstawie: EY, *Cybersecurity and the Internet of Things*, http://www.ey.com, dostęp 14.11.2016, s. 20.

Tabela 9. Przeszkody dotyczące skuteczności ochrony informacji

Wyszczególnienie	Udział w %
Ograniczenia budżetowe	62
Brak wykwalifikowanych zasobów	57
Brak świadomości wykonawczej lub wsparcia	32
Brak odpowiedniej jakości narzędzi do zarządzania bezpieczeństwem informacyjnym	28
Brak prawidłowego zarządzania	28
Fragmentacja dotycząca regulacji zgodności	23
Inne	7

Źródło: jak pod tab. 4, s. 26.

Z przedstawionych w tabeli 9 rezultatów badań wynika, że największą barierą jest przeznaczenie zbyt małego budżetu na bezpieczeństwo informacji. Potwierdzają to badania przeprowadzone przez PwC, z których wynika, że firmy polskie przeznaczają zaledwie 10% budżetu przeznaczonego na IT na cyberbezpieczeństwo

w stosunku do 19% na świecie[24]. Następne bariery dotyczą czynnika ludzkiego, a przede wszystkim braku osób z odpowiednimi kwalifikacjami (57%), a w następnej kolejności jest brak świadomości dotyczących zagrożeń komputerowych (32%). Istotnymi barierami są również brak skutecznych narzędzi i nieprawidłowa organizacja systemu bezpieczeństwa cybernetycznego.

W związku z rozwojem technologii, a w ślad za tym również technik przestępczości, same organizacje bardzo często nie są w stanie sobie z tym poradzić. Niewiele z nich posiada pracowników z odpowiednimi umiejętnościami i zasoby, które umożliwiałyby skuteczne zabezpieczenie firmy przed zagrożeniami wynikającymi z przestępczości komputerowej. Rozwiązaniem tego problemu może być współpraca z innymi organizacjami tej samej branży[25] bądź skorzystanie z zewnętrznego wsparcia, jakie można uzyskać od firm, które posiadają wysoko wykwalifikowanych pracowników[26], duże doświadczenie pozyskane w różnych branżach oraz odpowiednie narzędzia organizacyjne i techniczne.

Przykłady usług dotyczących rachunkowości śledczej i cyberbezpieczeństwa, których zadaniem jest obrona przed cyberatakami, ich wykrywanie, przygotowywanie odpowiednich procedur i kształtowanie kultury organizacyjnej bardziej otwartej w cyberprzestrzeni, a jednocześnie odpornej na przestępczość komputerową, przedstawiono w tabeli 10.

Przedstawione w tabeli 10 usługi można zaliczyć do rachunkowości śledczej. Wyspecjalizowane firmy oferują szeroki zakres usług, w celu przygotowania organizacji na cyberataki, jak również budowania sformalizowanej struktury bezpieczeństwa cybernetycznego. Polska należy do krajów o niskim poziomie cyberbezpieczeństwa w porównaniu z organizacjami światowymi. Obecnie w Polsce sformalizowany system zabezpieczeń ma 46% firm w stosunku do firm światowych, gdzie ma je 91% organizacji[27].

Dodatkowym zabezpieczeniem przed skutkami cyberataków mogą być ubezpieczenia dotyczące ich skutków, które mogłyby zminimalizować szkody powstałe w wyniku tego typu incydentów. W Polsce ten typ zabezpieczeń nie jest jeszcze zbyt powszechny, w badaniach przeprowadzonych przez PwC zaledwie 8% firm

[24] PWC, *W obronie...*, op.cit., s. 7.

[25] Z badań przeprowadzonych przez PWC wynika, że 45% organizacji nawiązuje taką współpracę, PwC, *W obronie...*, op.cit., s. 18.

[26] Por. K.T. Smith, L.M. Smith, J.L. Smith, *Case Studies of Cybercrime and Their Impact on Marketing Activity and Shareholder Value*, „Academy of Marketing Studies Journal" 2011, vol. 15, no. 2, s. 76.

[27] PwC, *W obronie...*, op.cit., s. 9.

biorących udział w badaniu zadeklarowało zawarcie polisy ubezpieczeniowej od następstw cyberataków, natomiast w przypadku badań światowych takie ubezpieczenie zakupiło 59% firm[28].

Tabela 10. Przykłady usług dotyczących cyberbezpieczeństwa

Rodzaj oferowanej usługi	Przykładowy zakres działań
Informatyka śledcza	• Stworzenie planu i zarządzanie procesem zabezpieczenia dysków twardych, taśm i dowodów cyfrowych, zgodnie z zasadami zabezpieczania materiału dowodowego • Odszukanie i gromadzenie danych elektronicznych, niezależnie od tego, gdzie się znajdują • Odtwarzanie historycznego stanu danych – przywracanie bazy danych systemu finansowego do stanu z przeszłości w poszukiwaniu dowodów popełnienia nadużyć • Identyfikacja, odzyskiwanie, zabezpieczanie oraz analiza dowodów elektronicznych zapisanych na różnego rodzaju nośnikach oraz w dowolnej konfiguracji • Przeanalizowanie materiału dowodowego w celu zlokalizowania, identyfikacji i wydobycia informacji mającej wartość dla dochodzenia lub sporu • Wykrywanie przypadków korupcji oraz malwersacji finansowych • Ujawnienie manipulacji sprawozdawczością finansową • Identyfikacja kradzieży majątku • Identyfikacja oszustw pracowniczych • Identyfikacja kradzieży danych • Ujawnienie konfliktów interesu (pracownicy – dostawcy) • Identyfikacja pracowników zamieszanych w oszustwa • Rozszerzenie wiedzy odnośnie do ryzyka, na które narażona jest spółka • Zbieranie publicznie dostępnych informacji o podmiotach i osobach, sposobach oraz strategiach działania osób i podmiotów stanowiących przedmiot zainteresowania klientów
Śledcza analiza danych	• Przeprowadzanie zaawansowanych analiz danych w zakresie dużych wolumenów transakcji i danych zawartych w systemach finansowo-księgowych, systemach CRM oraz systemach naliczania i wypłaty prowizji, w celu identyfikacji zdarzeń niewidocznych przy wykorzystaniu innego typu analiz • Badanie jakości i spójności danych, w tym analiza praktyk zarządzania danymi • Odnajdywanie zależności między pozornie niepowiązanymi źródłami danych • Identyfikacja sygnałów ostrzegawczych, które mogą świadczyć o wystąpieniu nadużyć • Analiza i mapowanie ryzyka w poszczególnych obszarach na podstawie indywidualnie dobranych kryteriów • Przewidywanie zagrożeń przyszłych nadużyć na podstawie analizy danych historycznych

[28] Ibidem, s. 18.

Rodzaj oferowanej usługi	Przykładowy zakres działań
Odzyskiwanie usuniętych danych i przeszukiwanie zbiorów komputerowych	• Zabezpieczanie elektroniczne danych komputerów, tabletów oraz telefonów komórkowych • Odzyskiwanie usuniętych informacji oraz ich szczegółowa analiza
Wdrażanie nowych narzędzi	• Wsparcie we wdrażaniu technologii służącej minimalizowaniu ryzyka nadużyć oraz prania pieniędzy
Cyberbezpieczeństwo	• Wykrywanie i odpowiedź na cyberzagrożenia • Ocena istniejącego środowiska bezpieczeństwa • Budowanie programu ochrony cybernetycznej – ochrona danych i prywatności • Zarządzanie cyberbezpieczeństwem

Źródło: opracowanie własne na podstawie: Deloitte, *Usługi. Zarządzanie ryzykiem nadużyć i zgodnością*, http://www2.deloitte.com/pl, dostęp 9.03.2016; E&Y, *Zarządzanie ryzykiem nadużyć*, http://www.ey.com/PL/pl, dostęp 8.03.2016; KPMG, *Zarządzanie ryzykiem nadużyć*, http://www.kpmg.com/PL/pl, dostęp 9.03.2016; PwC, *Usługi Forensic*, http://www.pwc.pl, dostęp 9.03.2016.

5. Podsumowanie

Cyberprzestępczość stanowi zagrożenie dla każdej, nawet najmniejszej organizacji. Poszczególne jednostki posiadają informacje, które mogą być atrakcyjne dla potencjalnego przestępcy. Przestępczość komputerowa zatem dotyczy każdej jednostki, natomiast dotychczasowe badania nad cyberprzestępczością dotyczyły w przeważającej części tylko największych organizacji, zatem nie odpowiadają one rzeczywistej skali tego zjawiska. Szczególnie odnosi się do specyfiki polskiego rynku, gdzie 99,8% jednostek stanowią małe i średnie przedsiębiorstwa[29]. Dla przedstawienia wielkości strat, jak również sposobów przeciwdziałania tego typu zjawiskom dalsze badania dotyczące Polski powinny objąć również przedsiębiorstwa sektora małych i średnich przedsiębiorstw.

W dobie cyfrowego świata działalność gospodarcza, dzięki postępowi technicznemu i stosowaniu różnych narzędzi, takich jak: urządzenia mobilne, Internet, media społecznościowe czy też chmury obliczeniowe, staje się bardziej otwarta, nie jest chroniona żadnymi granicami. Zdobycze techniki są z jednej strony lokomotywą rozwoju przedsiębiorstw, z drugiej stają się narzędziem w rękach przestępców. Zagrożenia wynikające z zastosowania nowoczesnych technologii wymuszają na ustawodawcach uchwalanie uregulowań prawnych, uwzględniających powstawanie

[29] PARP, *Raport o stanie sektora MSP w Polsce*, Polska Agencja Rozwoju Przedsiębiorczości, https://www.parp.gov.pl, dostęp 18.07.2017, s. 7.

coraz to nowszych rodzajów nadużyć z użyciem nowoczesnych technologii. Ponadto wymuszają na przedsiębiorstwach wprowadzenie rozwiązań systemowych dotyczących bezpieczeństwa informacji w celu ograniczenia występowania tego typu incydentów i zminimalizowania strat powstałych w ich wyniku. W Polsce brak jest badań dotyczących wpływu uregulowań prawnych na cyberataki oraz na wprowadzanie przez przedsiębiorstwa nowych rozwiązań systemowych.

W świecie cyfryzacji i globalizacji cyberbezpieczeństwo przestało być trendem, natomiast stało się strategiczną koniecznością każdej organizacji[30].

Bibliografia

Dokumenty prawne

1. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW, Dz.U. UE L 218 z dnia 14.08.2013 r.
2. Ustawa z dnia 29 września 1994 r. o rachunkowości, Dz.U. z 2016 r., poz. 1047 ze zm.
3. Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, Dz.U. z 2003 r., nr 153, poz. 1503 ze zm.
4. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, Dz.U. z 1997 r. nr 88, poz. 553 ze zm.
5. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. z 2015 r., poz. 2135 ze zm.

Wydawnictwa zwarte

1. Barclay C., *Using Frugal Innovations to Support Cybercrime Legislations in Small Developing States: Introducing the Cyber-Legislation Development and Implementation Process Model (CyberLeg-DPM)*, „Information Technology for Development" 2014, vol. 20, no. 2.
2. Brzezin W., *Ogólna teoria rachunkowości*, Wyższa Szkoła Handlu i Prawa, Warszawa 1998.
3. Brzezin W., *Rachunkowość sensu stricto i sensu largo*, „Zeszyty Teoretyczne Rachunkowości" 2000, t. 56.
4. Burzym E., *Rachunkowość przedsiębiorstwa i instytucji*, PWE, Warszawa 1980.
5. Hendriksen E.A., van Breda M.F., *Teoria rachunkowości*, Wydawnictwo Naukowe PWN, Warszawa 2002.

[30] PwC, *W obronie...*, op.cit., s. 1.

6. Hui K.L., Kim S.H., Wang Q.H., *Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks*, „MIS Quarterly" 2017, vol. 41, no. 2.
7. Jabłoński A., Kawczyńska M., Pietrzak Ż., Wnuk-Pel T., *Oczekiwany wpływ implementacji zintegrowanego systemu informatycznego na jakość informacji – studium przypadku*, „Zeszyty Teoretyczne Rachunkowości" 2016, t. 89(145).
8. Jarugowa A., *Niektóre wyznaczniki rozwoju rachunkowości*, w: *Współczesne problemy rachunkowości*, red. A. Jarugowa, PWE, Warszawa 1991.
9. Jarugowa A., *Wprowadzenie – istota zmian w ustawie o rachunkowości i ich skutki ekonomiczne*, w: *Komentarz do ustawy o rachunkowości. Rachunkowość – MSR – Podatki*, red. A. Jarugowa, T. Martyniuk, Ośrodek Doradztwa i Doskonalenia Kadr, Gdańsk 2002.
10. Kshetri N., *Positive Externality, Increasing Returns, and the Rise in Cybercrimes*, „Communications of the ACM" 2009, vol. 52, no. 12.
11. Kunz B., Tymińska A., *System informatyczny rachunkowości i jego rola w świetle ustawy o rachunkowości*, „Nauki o Finansach" 2014, nr 3(20).
12. Mayer J., *Cybercrime Litigation*, „University of Pennsylvania Law Review" 2016, vol. 164.
13. Skrzywan S., *Rachunkowość w przedsiębiorstwie przy gospodarce planowej. Cele i funkcje*, Prace Zakładu Rachunkowości SGH w Warszawie, nr 1, Gospodarczy Instytut Wydawniczy, Warszawa 1948.
14. Smith K.T., Smith L.M., Smith J.L., *Case Studies of Cybercrime and Their Impact on Marketing Activity and Shareholder Value*, „Academy of Marketing Studies Journal", 2011, vol. 15, no. 2.
15. Sojak S., *Pojęcie rachunkowości*, w: *Podstawy rachunkowości*, red. S. Sojak, J. Stankiewicz, TNOiK, Toruń 2008.
16. Turyna J., *Rachunkowość finansowa*, C.H. Beck, Warszawa 2005.
17. Walińska E., *Międzynarodowe Standardy Rachunkowości*, Oficyna Ekonomiczna, Kraków 2006.
18. Wells J.T., *Nadużycia w firmach. Vademecum. Zapobieganie i wykrywanie*, LexisNexis, Warszawa 2006.

Materiały internetowe

1. Deloitte, *Beneath the Surface of a Cyberattack. A Deeper Look at Business Impacts*, https://www2.deloitte.com
2. Deloitte, *Usługi. Zarządzanie ryzykiem nadużyć i zgodnością*, http://www2.deloitte.com/pl
3. EY, *Creating Trust in the Digital World. EY's Global Information Security Survey 2015*, http://www.ey.com

4. EY, *Cybersecurity and the Internet of Things*, http://www.ey.com
5. EY, *Megatrends 2015. Making Sense of a Word in Motion*, http://www.ey.com
6. EY, *Zarządzanie ryzykiem nadużyć*, http://www.ey.com/PL/pl
7. Góra J., *Raport. Efektywne zarządzanie bezpieczeństwem informacji*, Ślązak, Zapiór i Wspólnicy, Media Recowery, https://www.us.edu.pl
8. KPMG, *Cyberbezpieczeństwo – wyzwanie współczesnego prezesa*, https://assets.kpmg.com
9. KPMG, *Future State 2030: Światowe wyzwania dla liderów i przywódców*, https://www.kpmg.com/PL/pl/
10. KPMG, *Profil korporacyjnego oszusta*, https://assets.kpmg.com
11. KPMG, *Zarządzanie ryzykiem nadużyć*, http://www.kpmg.com/PL/pl
12. PARP, *Raport o stanie sektora MSP w Polsce*, Polska Agencja Rozwoju Przedsiębiorczości, https://www.parp.gov.pl
13. PwC, *Usługi Forensic*, http://www.pwc.pl
14. PwC, *W obronie cyfrowych granic, czyli 5 rad, aby realnie wzmocnić ochronę firmy przed CYBER ryzykiem*, https://www.pwc.pl

Information Security and Computer Crime Risk

Summary

The development of new technologies and the global market affect the surrounding reality. It is the computer systems, including the IT accounting systems that evolve especially dynamically. Accounting, as one of the most important elements of the information system of a business entity is particularly exposed to the threats resulting from the development of modern computer technologies and the global market. The article aims at the presentation of legal regulations as well as threats to the business pursuit resulting from the development of new technologies, in particular to the corporate information systems as well as the methods of their detection and prevention. At the age of continuous cyberattacks, it is essential to pursue immediate and efficient actions in order to prevent such threats to synchronise technology, legal procedures and communication management. Cybersecurity has become a sheer necessity in view of such a dynamic development of modern technologies.

Keywords: accounting, computer crime, forensic accounting, cybersecurity