Maria Ewa Szatlach

PODWÓJNA WIRTUALNOŚĆ GOSPODARKI NIEOFICJALNEJ

Jednym z charakterystycznych zjawisk współczesnej gospodarki światowej jest szybki rozwój gospodarki nieoficjalnej (nieformalnej, czarnej, nierejestrowanej czy szarej) (Schneider 2005: 113–129; Feige 1989: 1–5). Mimo że wywiera ona olbrzymi wpływ na gospodarki narodowe i gospodarkę światową, nie podlega żadnej kontroli organów administracji państwowej czy instytucji międzynarodowych, nie występuje w żadnych oficjalnych statystykach i nie jest uwzględniana w PKB. Niektóre nierejestrowane formy działalności gospodarczej, takie jak handel narkotykami, są nielegalne, natomiast inne, jak na przykład sąsiedzka wymiana usług czy prace domowe, są legalne, lecz mogą zawierać w sobie niedozwolony element w postaci niezarejestrowanej zapłaty. W gospodarce nieoficjalnej istnieją również formy całkowicie legalne, jak na przykład produkcja na własne potrzeby. Ponieważ gospodarka nieformalna nie figuruje w oficjalnych rejestrach, jej oszacowanie sprawia wiele problemów, które nasiliły się szczególnie w ostatnich dwóch dekadach, co przypisywane jest procesom globalizacji we współczesnym świecie (Chomsky 2000: 723–737).

Zdefiniowanie pojęcia **gospodarka nieoficjalna** stało się sporym wyzwaniem, ponieważ – jak już wspomniano – ma ona znaczące i w zasadzie niekwestionowane implikacje dla gospodarki oficjalnej. Brak konsensusu w sformułowaniu ujednoliconej definicji sprawia, że ważne pytania typu: „Na ile gospodarka ta wypacza oficjalne dane makroekonomiczne?", „Czy można oszacować całą działalność w szarej strefie?", „Jaki jest rozmiar gospodarki nieoficjalnej w państwach o różnych poziomach rozwoju?", itp., wciąż pozostają bez odpowiedzi (Fleming, Roman, Farrell 2003: 388).

Bogdan Mróz wyróżnił dwie podstawowe definicje gospodarki nieoficjalnej. W ujęciu węższym do gospodarki nieformalnej zaliczył te sfery aktywności

gospodarczej, które powinny być, a nie są, objęte systemem rejestracji i kontroli instytucji państwowych (jak np. praca na czarno, nielegalny handel, wszelkie transakcje bez wystawienia faktury czy oszustwa podatkowe). W ujęciu szerszym do gospodarki nieformalnej zaliczył wszystkie rodzaje aktywności gospodarczej, które nie są objęte systemem rejestracji i nie znajdują odzwierciedlenia w PKB. W tym kontekście jest to nierejestrowana działalność gospodarcza o charakterze legalnym (np. sąsiedzka wymiana usług, samozaopatrzenie gospodarstw domowych), półlegalnym (wytwarzanie dóbr i usług niezabronionych przez obowiązujące przepisy, ale ukryte przed urzędami podatkowymi) oraz nielegalnym, bardzo często przestępczym (wytwarzanie dóbr i usług zabronionych przez regulacje i przepisy prawne) (Mróz 2002: 14–25). Według Anny Krajewskiej termin „gospodarka nieoficjalna" oznacza działalność ekonomiczną prowadzoną poza rejestracją i regulacją państwa, a więc nieobjętą opodatkowaniem. Do szarej strefy zalicza ona zarówno dochodowe działania podejmowane zgodnie z prawem, ale niezgłoszone do urzędu skarbowego, jak i działania z pogranicza prawa, a także działalność przestępczą – nielegalną (Krajewska 2004: 237). Według kryminologa, Brunona Hołysta, gospodarka nieoficjalna jest całością nieewidencjonowanych działań gospodarczych i zarobkowych oraz osiąganych z nich dochodów pozostających poza kontrolą fiskalną aparatu państwowego (Hołyst 1997: 323). Z kolei Bruno S. Frey i Friedrich Schneider postrzegają gospodarkę nieoficjalną jako część gospodarki nie zarejestrowanej w PKB, co powoduje brak adekwatnej wiedzy na temat wpływu szarej strefy na gospodarkę narodową oraz liczby zatrudnionych w niej osób (Frey, Schneider 2001: 35). Natomiast według przyjętego w 1993 r. Systemu Rachunków Narodowych ONZ gospodarka nieoficjalna składa się z produkcji nielegalnej oraz produkcji ukrytej (Rajewski, Zienkowski 1994: 3–6).

Gospodarka nieoficjalna jest nie tylko trudna do analizy, ale i do oceny, a jej efekty mogą być zarówno pozytywne (np. przyczynia się do ożywienia gospodarczego, pozytywnie stymuluje oficjalną gospodarkę, otwiera możliwości powstawania nowych miejsc pracy oraz zwiększa podaż towarów i usług na rynku), jak i negatywne (np. zniekształca statystyczny obraz całej gospodarki narodowej, regionalnej i światowej, osłabia prestiż państwa w oczach obywateli, powoduje zmniejszenie potencjalnych dochodów budżetu państwa, oddziałuje także na mentalność i postawy ludzi zacierając granicę między przedsiębiorczością a kombinatorstwem, tym, co naganne, a co dopuszczalne) (Kozłowski 2004: 7–8; Schneider, Enste 2000: 20–25; Gikas 1992).

Większość wyników badań na temat gospodarki nieoficjalnej wykazuje, że główną przyczyną jej powstania są obciążenia podatkowe. Potrzeba ponoszenia obciążeń podatkowych jest dla obywateli, co do zasady, zrozumiała w sytuacji, kiedy państwo wywiązuje się ze swoich obowiązków i nie dochodzi do marnotrawstwa środków publicznych. Podwyższanie podatków powoduje jednak reakcje obronne i podatnicy zaczynają szukać rozwiązań

umożliwiających ich zmniejszenie. Często są to rozwiązania nielegalne związane z ukrywaniem dochodów i popełnianiem oszustw podatkowych (Ćwikowski 2012: 305). W wielu przypadkach niepłacenie podatków może mieć związek z wysokim poziomem korupcji w instytucjach odpowiedzialnych za ich pobór, przymykaniem oczu na nieprawidłowości w rozliczeniach podatkowych, brakiem skutecznej kontroli oraz wydawaniem korzystnych decyzji i interpretacji przepisów (tamże: 311). Najbardziej jaskrawym przykładem oszustwa podatkowego jest ukrywanie przedmiotu opodatkowania, czyli niezgłaszanie do właściwych organów działalności gospodarczej, jak i zatajenie przed urzędem podatkowym pojedynczych transakcji (pożyczek gotówkowych, sprzedaży rzeczy używanych o znacznej wartości) oraz wykonywania dorywczo usług dla ludności, a także prac sezonowych na czarno. Typowym sposobem unikania opodatkowania jest nieewidencjonowanie przychodów i w konsekwencji dochodów z prowadzonej działalności zarobkowej. Dotyczy to osób prowadzących działalność gospodarczą małych i średnich rozmiarów na targowiskach, w gastronomii, branży budowlanej, hotelarskiej oraz świadczących usługi (naprawcze, korepetycje). Jedną z przyczyn nieujawniania dochodów są niezbyt restrykcyjne i niedoskonałe przepisy dotyczące obowiązku rejestrowania przychodów do celów podatkowych. Oprócz zaniżania przychodów osoby fizyczne i prawne dokonują nieprawidłowości kwalifikacji części wydatków jako kosztów uzyskania przychodów. Organy kontrolne nie są w stanie udowodnić, jaka część wydatków osobistych nie dotyczy prowadzonej działalności. Z zaniżaniem przychodów i dochodów podatników łączy się bezpośrednio zatrudnienie na czarno. Taką pracę wykonują osoby w różnym wieku, najczęściej słabo wykształcone (w usługach budowlanych, drobnych usługach dla ludności, handlu bazarowym, usługach sąsiedzkich, turystycznych i gastronomicznych) (Ćwikowski 2012: 313–318).

Kolejnym ważnym czynnikiem wpływającym na wielkość gospodarki nieoficjalnej jest wzrost intensywności regulacji (mierzony ilością przepisów i regulacji prawnych), który redukuje zakres wolności wyboru podmiotów gospodarczych w gospodarce oficjalnej. Generalnie, im większa ilość regulacji w gospodarce, tym więcej ludzi stara się je w jakiś sposób obejść. Regulacje dotyczą rynku dóbr (np. kontrola cen, racjonowanie towarów, kontyngenty importowe i eksportowe), rynku finansowego (kształtowanie stóp procentowych, kontrola udzielania kredytów) oraz rynku pracy (wprowadzanie przepisów w zbyt dużym stopniu ograniczających swobodę działań pracodawców, zmniejszanie ilości godzin pracy, określanie poziomu płac minimalnych, ograniczanie pracy w godzinach nadliczbowych i zbyt rozbudowany system przyznawania zasiłków dla bezrobotnych) (Johnson, Kaufman, Zoida-Lobaton 1998: 387–392).

Charakter gospodarki nieoficjalnej sprawia, że jej uchwycenie i oszacowanie jest niezwykle trudne. Różne metody badań prowadzą do znacznie zróżnicowanych wyników. W badaniach empirycznych stosuje się najczęściej trzy metody mierzenia jej rozmiarów. W podejściu związanym z popytem

na pieniądz (*currency demand approach*) zakłada się, że transakcje w gospodarce nieoficjalnej realizowane są w formie zapłat gotówkowych, żeby nie zostawiać widocznych śladów dla urzędów skarbowych (i innych instytucji państwowych). Według założeń tej metody wzrost aktywności gospodarki nieoficjalnej powoduje wzrost popytu na pieniądz. Aby odizolować wynik **nadwyżki** popytu na pieniądz, spowodowany działalnością podmiotów w gospodarce nieoficjalnej, jej autorzy korzystają z ekonometrycznego równania szacunkowego, zawierającego wszystkie konwencjonalne czynniki, takie jak wzrost dochodu, zmiany w warunkach płatności, pośrednie i bezpośrednie obciążenia podatkowe, regulacje rządowe i obciążenia związane ze sferą socjalną. **Dodatkowy** wzrost popytu na pieniądz, niewytłumaczalny przez czynniki tradycyjne, jest zatem przypisany szarej strefie, przy założeniu, że prędkość obiegu pieniądza w gospodarce formalnej i nieformalnej jest taką samą wielkością. Dynamiczne podejście za pomocą modelu DYMIMIC (*DYMIMIC model*) jest jedną z metod wieloczynnikowych i bierze pod uwagę szeroki wachlarz przyczyn, powodujących powstanie, funkcjonowanie i wzrost gospodarki nieoficjalnej, jak również efekty tej gospodarki. Metoda ta bazuje na statystycznej teorii nieobserwowalnych zmiennych (*theory of unobserved variables*). Trzecia metoda, związana z zużyciem energii elektrycznej (*physical input – electricity consumption method*), zakłada, że część jej dostaw zużywana jest w gospodarce nieformalnej i że można oddzielić tę wielkość oraz wyliczyć wielkość wartości dodanej w gospodarce nieoficjalnej. Zużycie energii elektrycznej porównywane jest z oszacowanym spodziewanym poziomem zużyciem energii oraz poziomem PKB. Podejście to zakłada, że stosunek zużycia energii elektrycznej i uzyskanego poziomu PKB może być oszacowany za pomocą metod ekonometrycznych, a różnice w spodziewanych poziomach przypisywane są działalności w gospodarce nieoficjalnej (Jarociński 1995: 49–66).

Procesy globalizacji, intensyfikujące powiązania gospodarcze w skali całego świata, powodują pojawianie się nowych sfer gospodarki nieoficjalnej oraz nowych możliwości jej ekspansji. W ostatnich latach zauważalny jest szybki wzrost jednego z jej segmentów o charakterze przestępczym, mianowicie kryminalnego podziemia gospodarczego (Goglio 2004: 853–865). Odzwierciedleniem tego procesu jest wzrastająca liczba międzynarodowych przestępstw gospodarczych oraz pojawienie się nowych trendów i zjawisk zmieniających oblicze współczesnej zorganizowanej przestępczości gospodarczej. Nastąpił proces jej umiędzynarodowienia z wykorzystaniem środków i metod stosowanych w oficjalnym biznesie (np. porozumienia o współpracy, fuzje, sojusze i alianse strategiczne w różnych układach i przekrojach między międzynarodowymi grupami przestępczymi). Do działań przestępczych zatrudnia się wysokiej klasy fachowców z zakresu prawa finansowego i podatkowego oraz informatyków. Grupy przestępcze dysponują obecnie supernowoczesnym zapleczem technologicznym, pozwalającym na planowanie i realizowanie operacji w globalnym wymiarze (Mróz 2002: 85). Międzynarodowa przestępczość zorganizowana

charakteryzuje się wysoką przedsiębiorczością, polegającą na zorganizowaniu odpowiedniego marketingu, zaopatrywaniu się w półprodukty oraz posiadaniu sieci sprzedaży hurtowej i detalicznej. Grupy przestępcze poszukują takich segmentów gospodarki, które niosą najmniejsze ryzyko wykrycia, wymagają mniejszego wysiłku i niższych kosztów oraz zapewniają szybki i łatwo osiągalny zysk. Członkowie tych grup charakteryzują się dużym profesjonalizmem, związanym z wykorzystaniem nowoczesnych środków komunikacji i łączności, przetwarzaniem i przesyłaniem danych oraz korzystaniem z Internetu. Współczesne międzynarodowe grupy przestępcze działają w sposób systematyczny, zdyscyplinowany i skoordynowany, z wyłączeniem wszelkich motywów emocjonalnych. Działają w głębokiej konspiracji, stosując w swojej działalności zastraszenie i przemoc oraz korumpowanie przedstawicieli administracji publicznej bądź samorządowej. Cechuje je daleko posunięty internacjonalizm, wyrażający się dużą mobilnością ponadregionalną. Uzyskały też ochronę prawną legalnych firm prawniczych, dzięki czemu są w stanie gromadzić i kumulować kapitał (Jasiński 2001: 24–29).

Przestępczość zorganizowaną definiuje się jako każdą grupę osób na stałe zaangażowaną w prowadzenie niezgodnej z prawem działalności, której głównym celem jest pomnażanie zysków przy jednoczesnym naruszaniu międzypaństwowych granic i przepisów celnych (Gilmore 1999: 21). Państwowa Służba Wywiadu Kryminalnego Wielkiej Brytanii (National Criminal Intelligence Service – NCIS) uwzględnia cztery główne kryteria: grupowe działanie, główny cel – zysk finansowy, długi okres i ciągłość nielegalnych działań, międzynarodowy charakter operacji z naruszeniem granic państwowych, oraz trzy kryteria uzupełniające: dużą skalę operacji, przeznaczenie dochodów uzyskanych z nielegalnego procederu na cele niezgodne z prawem oraz strukturę grupy i dyscyplinę jej członków (Gilmore 1999: 22). Współczesne grupy przestępcze specjalizują się w określonych rodzajach nielegalnej działalności. Opanowały nie tylko tradycyjne dziedziny, takie jak: podrabianie produktów znanych marek i towarów ekskluzywnych (Goławska 2002: 36–40), korupcję w sektorze publicznym (nielegalne opłacanie urzędników publicznych w zamian za korzyści uzyskiwanie dzięki ich decyzjom) (Kozłowski 2004: 85–90), gry hazardowe, wymuszanie – wyłudzanie, prostytucję, wszelkiego typu fałszerstwa, oszustwa bankowe (udzielanie kredytów dla nieistniejących podmiotów gospodarczych i osób, udzielanie fikcyjnych gwarancji bankowych, wyłudzanie kredytów na podstawie przywłaszczonego wcześniej majątku, nieprzestrzegania przepisów przez pracowników banków, współdziałanie pracowników banków z przestępcami oraz fałszowanie dokumentów bankowych) (Laskowska 2011: 124), nielegalny handel bronią, ale też i bardziej nowoczesne: handel chronionymi gatunkami zwierząt, nielegalny transport i składowanie odpadów chemicznych, kradzież technologii, niszczenie systemów komputerowych, oszustwa komputerowe, oszustwa inwestycyjne (niezwracanie

inwestorom zainwestowanych pieniędzy)[1], piramidy finansowe (przedsięwzięcia, w których środki finansowe kolejnych inwestorów są wykorzystywane do regulowania zobowiązań wobec osób, które dołączyły do nich jako pierwsze), szpiegostwo gospodarcze, przestępstwa celne i dewizowe (świadome unikanie płacenia świadczeń pieniężnych na rzecz Skarbu Państwa, takich jak cło, podatki i inne opłaty obowiązkowe)[2], fikcyjne bankructwa[3], oszustwa ubezpieczeniowe (zgłaszanie nienależnych, wielokrotnych lub zawyżonych roszczeń lub celowe zniszczenie przedmiotu ubezpieczenia)[4], piractwo dóbr intelektualnych, przemyt nielegalnych imigrantów, handel materiałami rozszczepialnymi, handel organami ludzkimi, kradzież

---

[1] Dynamiczny rozwój Internetu otworzył nowe perspektywy i obszary działań dla oszustw inwestycyjnych. W sieci znajduje się mnóstwo informacji na temat rynków finansowych i różnorodnych możliwości inwestycyjnych na całym świecie. Komputerowi oszuści często posługują się tzw. akcjami za centa (*penny stocks*), czyli papierami o wartości kilku centów, emitowanymi przez niewielkie i małe firmy (Gilmore 1999: 21–22).

[2] Przestępczość ta rozwija się w następujących dziedzinach: przewożenie towarów poza kontrolą celną, czyli przemyt; oszustwa celne związane z ilością, rodzajem i wartością towaru, co związane jest z możliwością zastosowania niższej stawki celnej; fałszowanie świadectw pochodzenia towaru w celu uzyskania preferencji celnych; fikcyjny reeksport towarów w celu zwrotu pobranego cła od towarów, który faktycznie pozostał w kraju; fikcyjny wywóz za granicę surowców w celu rzekomego przetworzenia lub uszlachetnienia i sprowadzenie w to miejsce towarów wyprodukowanych za granicą; fikcyjny tranzyt – zgłoszenie wprowadzenia towarów na obszar celny w transporcie do innego państwa i pozostawienie ich w kraju, dzięki czemu nie uiszcza się opłat celnych i podatkowych; import towarów przez fikcyjnego odbiorcę bez dokonywania odprawy celnej lub fałszowanie odprawy celnej; stosowanie podwójnej dokumentacji (Laskowska 2011: 129).

[3] Fikcyjne bankructwa polegają na nieustannym przepływie aktywów do nowo powstających spółek na całym świecie, które celowo zakładają zobowiązania przekraczające możliwości ich spłacenia, a następnie upadają. Zakładane są też fasadowe firmy (*fly-by-night companies*), które znikają po zrealizowaniu jednej bądź kilku transakcji. Do najczęstszych technik stosowanych w przypadku fikcyjnych bankructw należą: zakładanie fikcyjnych filii i oddziałów oraz udzielanie im pożyczek, fikcyjny zakup środków trwałych i obrotowych, zakup środków trwałych za granicą z wykorzystaniem płatności w dwóch ratach: jednej adresowanej do sprzedającego, drugiej skierowanej na rachunek bankowy w wybranym kraju, fikcyjny zakup usług konsultingowych – (Mróz 2002: 86–115).

[4] W sektorze ubezpieczeń oszustwa polegają na wyłudzaniu nienależnych odszkodowań komunikacyjnych na podstawie upozorowanych lub umyślnie powodowanych kolizji drogowych. Polegają one najczęściej na: powodowaniu fikcyjnych zderzeń, zgłaszanych w zakładach ubezpieczeniowych; sprowadzanie uszkodzonych pojazdów z zagranicy, które wykorzystano w sfingowanej kolizji; fikcyjna kradzież luksusowych samochodów, które w rzeczywistości wywożone są do krajów Europy Środkowo-Wschodniej na podstawie oryginalnych dokumentów; upozorowanie kolizji i kradzieży z wykorzystaniem wraków samochodowych; antydatowanie polis ubezpieczeniowych. Poza wyłudzeniami odszkodowań komunikacyjnych dochodzi do wyłudzeń odszkodowań za sfingowane straty spowodowane pożarem, związane z ubezpieczeniami morskimi, kredytami bankowymi i transakcjami leasingowymi (Laskowska 2011: 130).

i przemyt samochodów oraz pranie pieniędzy (Gilmore 1999: 21–22). Wraz z globalizacją pojawił się przemyt związany z nieprzestrzeganiem przepisów dotyczących ochrony środowiska (składowanie niebezpiecznych odpadów, w tym radioaktywnych, substancji trujących i rakotwórczych, skażonego mięsa itp.) oraz nielegalny obrót towarami wysokoakcyzowymi (przemyt alkoholu i papierosów, brak kontroli nad wydawanymi pozwoleniami na ich przywóz, produkcja fałszywych banderoli, działania fikcyjne pozwalające na korzystanie z ulg i zniżek podatkowych, produkcja własna alkoholu) (Wysocki 2003: 34–35).

Migracja na wielką skalę z krajów rozwijających się do krajów Zachodu spowodowała powstanie gangów przestępczych o charakterze etnicznym i nacjonalistycznym. Grupy koreańskie, wietnamskie, chińskie, rosyjskie, karaibskie i południowoamerykańskie są dobrze zorganizowane w Stanach Zjednoczonych, Wielkiej Brytanii i Europie, a grupy przestępcze z Indii, Pakistanu, Sri Lanki i Bangladeszu – w krajach Zatoki Perskiej. W Singapurze sprawnie działają gangi przestępcze z Hong Kongu, Chin, Japonii i Malezji (Kim-Kwang Choo 2008: 271).

Warto w tym miejscu zwrócić szczególną uwagę na proceder prania pieniędzy, który obejmuje swym zasięgiem cały świat. Pranie brudnych pieniędzy oznacza wprowadzenie do obrotu środków pochodzących z działalności przestępczej. Problemem jest ich zalegalizowanie w obrocie finansowym. Najczęściej zakłada się rachunki bankowe na fikcyjne lub podstawione spółki. Na rachunkach tych lokuje się pieniądze, co ma potwierdzić ich legalne pochodzenie z określonej transakcji handlowej (najczęściej fikcyjnej). Na podstawie tej umowy pieniądze przekazywane są za granicę. Do prania pieniędzy wykorzystuje się zarówno banki, jak i instytucje finansowe – domy maklerskie, towarzystwa ubezpieczeniowe, fundusze inwestycyjne, a także rynek paliw płynnych i gazowych, obrót złomem i metalami kolorowymi oraz rynki: kapitałowy i nieruchomości. Pranie pieniędzy odbywa się też w przemyśle rozrywkowym (gry hazardowe, dyskoteki, organizowanie koncertów, agencje artystyczne). Ponadto proceder ten występuje w handlu nieruchomościami, dziełami sztuki, samochodami, obrocie towarami koncesjonowanymi, biżuterią, metalami szlachetnymi oraz towarami luksusowymi, w biurach turystycznych, usługach gastronomicznych, czyli tam, gdzie ułatwione jest wystawianie fałszywych faktur na dużą skalę, zaniżanie lub zawyżanie cen, uznawanie rzekomych reklamacji. W dobie Internetu i globalizacji pranie brudnych pieniędzy przybiera nowe formy, o czym będzie mowa w dalszej części pracy. Charakterystyczną tendencją ostatnich lat jest ogólnoświatowy zasięg tego zjawiska, coraz częstsze wykorzystywanie pozabankowych instytucji finansowych oraz profesji niefinansowych w operacjach **czyszczenia** brudnych pieniędzy (np. kancelarii prawniczych, agencji handlu nieruchomościami, branży turystycznej i gastronomicznej). We współczesnym świecie głównymi obszarami zagrożonymi praniem pieniędzy są między innymi: sektor bankowy (fałszowanie czeków,

kart płatniczych, wyłudzanie kredytów)[5], sfera usług materialnych i niematerialnych (np. fakturowanie fikcyjnych robót, fałszowanie dokumentów dotyczących zamówień publicznych, odszkodowania dla biur turystycznych), rolnictwo (wyłudzanie dopłat do preferencyjnych kredytów), gospodarka energetyczna, obrót paliwami i surowcami oraz sfera własności intelektualnej (nielegalna produkcja i dystrybucja płyt, piractwo komputerowe) (Jasiński 2001: 19). Wśród źródeł pochodzenia brudnych pieniędzy najczęściej wymienia się następujące przestępstwa gospodarcze: oszustwa podatkowe (VAT, akcyza, cło), przemyt różnych towarów, nielegalny obrót towarami, fikcyjny obrót złotem, kosmetykami i lekarstwami, wyłudzanie kredytów bankowych, oraz przestępstwa kryminalne: porwania ludzi i wymuszanie okupu, rozboje i wymuszenia rozbójnicze, kradzież i przemyt samochodów, produkcja i handel narkotykami, nielegalny handel bronią, handel materiałami rozszczepialnymi, przemyt dzieł sztuki, fałszowanie pieniędzy, nielegalny hazard, porwania, handel ludźmi i organami ludzkimi, nielegalny przemyt emigrantów, prostytucja i stręczycielstwo[6].

Współczesne zorganizowane grupy przestępcze coraz częściej korzystają z nowoczesnych technologii informatycznych, głównie Internetu. Rozwój sieci internetowej spowodował wzrost technologii bezprzewodowych i urządzeń mobilnych. Istniejąca synergia pomiędzy zorganizowaną przestępczością i cyberprzestrzenią, która zapewnia grupom przestępczym pewne poczucie bezpieczeństwa, wzmacnia ich możliwości organizacyjne i operacyjne. **Przestępczość high-tech** jest obszarem wielkich możliwości prowadzenia nowych typów przestępstw. Grupy przestępcze zaczęły doceniać technologie informacyjne i komunikacyjne w usprawnianiu, wzmacnianiu oraz identyfikowaniu nowych rodzajów działalności przynoszących nadzwyczajne zyski, jak: handel narkotykami, ludźmi, tajemnicami korporacyjnymi i tożsamością, defraudacja, wyłudzanie, pranie pieniędzy przy użyciu systemów płatności on-line, dystrybucja nielegalnych materiałów przez Internet, używanie Internetu jako rynku sprzedaży nielegalnych produktów farmaceutycznych i lekarstw oraz sprzedaży wszelkiego rodzaju podróbek znanych światowych firm odzieżowych i kosmetycznych (Kim-Kwang Choo 2008: 272–274).

Cyberprzestępczość określa się najczęściej jako działalność przestępczą realizowaną za pośrednictwem komputera i Internetu, począwszy od ściągania nielegalnych plików muzycznych do kradzieży milionów dolarów

---

[5] Obława na harcowników. *Forum*. 17–30 grudnia 2001: 36.

[6] Według krajów członkowskich Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy – FATF (*Financial Action Task Force*) pieniądze z handlu narkotykami są na pierwszym miejscu na liście wszystkich źródeł brudnych pieniędzy. Dalsze miejsca zajmują wszelkiego rodzaju oszustwa, przemyt, gry hazardowe oraz handel żywym towarem. Pod koniec lat 90. przez Polskę przerzucanych było ze Wschodu około 20 tysięcy kobiet i około 2 tysięcy chłopców rocznie. Za ich dostarczenie do domów publicznych w Europie Zachodniej dostawało się od 250 do 2 500 euro za jedną osobę (Wójcik 2001: 56; Laskowska 2011: 133).

z internetowych kont bankowych. Cyberprzestępczość oznacza również takie przestępstwa, jak tworzenie i rozpowszechnianie wirusów w innych komputerach lub przekazywanie poufnych informacji o firmie za pomocą sieci[7].

Cyberprzestępczość, mimo różnych określeń, jak dotąd nie posiada jednoznacznej definicji. Spowodowane jest to głównie złożonością tego pojęcia oraz różnymi rozwiązaniami legislacyjnymi poszczególnych państw, które nie doprowadziły do wypracowania wspólnego międzynarodowego wzorca. Jedna z często cytowanych definicji określa cyberprzestępczość jako nielegalne działania, w których przedmiotem przestępstwa jest komputer. Z kolei grupa ekspertów w ramach OECD przyjęła następującą definicję: **jest to nadużycie informacyjne niezgodne z prawem lub sprzeczne z etyką bądź nieautoryzowane, dotyczące automatycznego przetwarzania i/lub transmisji danych** (Ştefan 2011: 115).

Eksperci ONZ podzielili cyberprzestępstwa na dwie kategorie. W wąskim sensie są to przestępstwa komputerowe, czyli wszelkie nielegalne działania związane z operacjami elektronicznymi, wymierzone przeciwko bezpieczeństwu systemów komputerowych i danych procesowanych przez te systemy. W szerokim ujęciu są to przestępstwa dotyczące korzystania z komputerów, czyli wszelkie nielegalne działania popełnione za pomocą systemów lub sieci komputerowych, włączając w to między innymi nielegalne posiadanie i udostępnianie lub rozpowszechnianie informacji przy użyciu systemów lub sieci komputerowych (Shinder 2004: 35). W literaturze przedmiotu cyberprzestępczość często definiuje się jako działalność przestępczą, w której komputery lub sieć internetowa są głównymi narzędziami popełnienia przestępstwa. Mogą to być: kradzież, naruszenie praw własności, treści obsceniczne oraz ataki na strony instytucji i organizacji. Wskazuje się przy tym na takie cechy cyberprzestępczości jak: szeroki dostęp do sieci, łatwy dostęp do narzędzi hakerskich, dzielenie się informacjami z innymi kryminalistami w cyberprzestrzeni, korzystanie z usług doświadczonych hakerów oraz luki w narodowych systemach prawnych (Kshetri 2009: 141–144).

Cyberprzestępczość dzieli się na przestępstwa dokonywane przy użyciu przemocy (cyberterroryzm, napaść przez zastraszenie, cyberprześladowanie, pornografia dziecięca) oraz przestępstwa dokonywane bez przemocy. Przestępstwa bez dokonywania przemocy dotyczą następujących procederów:

- cyberwtargnięcia polegającego na uzyskaniu nieautoryzowanego dostępu do zasobów komputera lub sieci, ale bez zniszczenia danych (szpiegowanie – *snooping* – czytanie cudzych e-maili, dokumentów, stron www, na które wchodzi obserwowany użytkownik),

[7] Należy zwrócić uwagę, że komputery i Internet są coraz częściej wykorzystywane do popełnienia pospolitych przestępstw, takich jak prostytucja, stręczycielstwo, pornografia dziecięca, fałszerstwo, szantaż itp.

- cyberkradzieży polegającej na użyciu komputera lub sieci do kradzieży informacji, pieniędzy lub czegoś innego. Zalicza się do nich: malwersację (przywłaszczenie pieniędzy – np. pracownik korzystający z legalnego dostępu do listy płac zmienia dane i wypłaca sobie pieniądze przelewając je na swoje konto); nieuprawnione przywłaszczenie (modyfikacja dokumentów nadających prawo własności); szpiegostwo korporacyjne (przemysłowe) – kradzież tajemnic handlowych, np. danych finansowych, poufnych list klientów, opisu strategii marketingowej lub innych informacji służących do uzyskania przewagi konkurencyjnej; popełnienie plagiatu – kradzież czyjegoś oryginalnego tekstu i opublikowanie jako własnego; piractwo – nielegalne kopiowanie oprogramowania muzyki, filmów, sztuki, książek; kradzież tożsamości – danych osobowych innych użytkowników w celu popełnienia przestępstwa (użytkownicy są zachęcani do korzystania z witryn, które w rzeczywistości są fałszywe, e-przestępcy proszą o informacje osobiste, takie jak hasło logowania, nazwę użytkownika, numery telefonów, kart kredytowych i kont bankowych); internetowe gry hazardowe; internetowa sprzedaż leków i narkotyków (jest to wielki biznes nielegalnie prowadzony przez apteki on-line); internetowe pranie brudnych pieniędzy (posługiwanie się Internetem do ukrywania źródeł pochodzenia nielegalnych środków),
- cyberkontrabandy – czyli nielegalnego przesyłanie przez Internet informacji ściśle tajnych, jak np. technologii szyfrowania (Shinder 2004: 37–49).

Internet usprawnił większość tradycyjnych przestępstw i w ten sposób stał się jednym z najbardziej niebezpiecznych narzędzi w rękach cyberprzestępców. Większość narzędzi stosowanych przez hakerów i dostępnych on-line nie wymaga w zasadzie jakiegoś specjalnego doświadczenia. Społeczność cyberprzestępcza udziela sobie pomocy, a w niektórych krajach powstały nawet wyspecjalizowane szkoły hakerów. Wielu studentów tworzy pirackie programy, nielegalnie włamuje się do systemów komputerowych i wymienia informacje. Takie doświadczenia pomagają im wejść do świata cyberprzestępczości i dają im poczucie bezkarności. Według raportu *McAfee Virtual Criminology* z marca 2007 r. 88% studentów z uniwersyteckich kierunków informatycznych dokonało przynajmniej jednego nielegalnego działania on-line (Kshetri 2009: 141–144).

Przestępstwa komputerowe przybierają różne formy i mogą być dokonywane w dowolnym miejscu i czasie (Szwarc 2009: 356). Powszechnym przestępstwem jest *hacking* komputerowy, polegający na złamaniu elektronicznych systemów zabezpieczeń, włamaniu się do systemu komputerowego i pozyskaniu informacji przez osobę nieuprawnioną. W ramach *hackingu* wyróżnia się: *cracking* (zjawisko polegające na łamaniu zabezpieczeń sieciowych serwerów przed nielegalnym korzystaniem z programów), *sniffing* (węszenie – jest to wstępna faza ataku komputerowego polegająca na rozpoznaniu terenu, czyli zdobyciu hasła użytkownika i identyfikatora),

wirusy komputerowe (po ich wprowadzeniu praca na komputerze zostaje ograniczona lub całkowicie uniemożliwiona). Kolejnym przestępstwem jest podsłuch komputerowy, czyli posługiwanie się specjalnym urządzeniem wizualnym i podsłuchowym w celu pozyskania poufnych informacji. Z kolei bezprawne niszczenie informacji oraz sabotaż komputerowy oznaczają usuwanie, uszkodzenie, niszczenie lub zmienianie ważnych danych strategicznych (w obszarze bezpieczeństwa komunikacyjnego, obronności kraju, działalności państwowej i samorządowej). Przestępstwo przeciwko mieniu prywatnemu i publicznemu to z kolei kradzież programu komputerowego oraz jego paserstwo (przyjmowanie, nabywanie lub pobieranie jakiegoś programu ze strony internetowej). Oszustwo telekomunikacyjne (*phreaking*) polega na tańszym lub bezpłatnym prowadzeniu rozmów telefonicznych poprzez włamanie się do systemów telekomunikacyjnych. Kradzież karty płatniczej, która w naturalny sposób stała się obiektem zainteresowania hakerów, jest kolejnym przestępstwem (Szwarc 2009: 357–366). Wiąże się z nią fałszowanie, kopiowanie (*skimming*), korzystanie z kart zagubionych lub niedoręczonych, wyłudzanie na podstawie fałszywych danych (Jakubski 2006: 39–40). Z kolei trojan to skrót określający konia trojańskiego, czyli program, który z pozoru wykonuje użyteczne zadania, a w rzeczywistości inicjuje działania, które nie leżą w intencji uruchomiającego program i których użytkownik nie jest świadomy. Hakerzy często tworzą konie trojańskie w celu obejścia zabezpieczenia systemu. Trojan usuwa lub modyfikuje i przesyła pliki oraz instaluje inne programy lub wirusy. Natomiast wirusy są programami, które często instalują się bez wiedzy użytkownika i wykonują niepożądane operacje wyrządzające szkody. Wirusy potrafią się klonować oraz infekować inne systemy. Często rozsyła się je jako załącznik do poczty elektronicznej. Niektóre aktywują się zaraz po instalacji, inne czekają na ustaloną z góry datę i godzinę. Istnieją tysiące rodzajów wirusów – począwszy od wyświetlenia okna z komunikatem *Hi!*, a skończywszy na skasowaniu całej zawartości dysku. Istnieje jeszcze robak, czyli program, który przemieszcza się od jednego komputera do drugiego za pośrednictwem sieci. Robaki tworzą wiele kopii samych siebie i rozprzestrzeniają się poprzez sieć (Shinder 2004: 318–320).

Cyberprzestępcy stają się coraz bardziej wyrafinowani i szybko rozwijają nowe formy i metody działania, a żadne państwo czy organizacja międzynarodowa nie są w stanie stworzyć wiarygodnej bazy danych hakerów. Współcześni cyberprzestępcy różnią się od konwencjonalnych – większość z nich to młodzi ludzie, dobrze wykształceni i zatrudnieni w firmach komputerowych, którzy nie odpowiadają zwykłym profilom przestępców i dlatego trudniej ich schwytać. Zorganizowana przestępczość w cyberprzestrzeni inicjowana jest w krajach, które nie mają regulacji prawnych dotyczących przestępstw popełnianych w sieci. Na przykład Stany Zjednoczone nie mogły wnieść oskarżenia przeciwko hakerowi z Filipin, który w 2000 r. wypuścił wirus o nazwie *Love Letter*, ponieważ Filipiny nie miały wtedy regulacji prawnych zakazujących popełniania przestępstw w cyberprzestrzeni.

Problemem jest również niedostateczna współpraca międzynarodowa organizacji walczących z cyberprzestępczością. Na przykład Rosja i Stany Zjednoczone podpisały porozumienie o współpracy w wykrywaniu zorganizowanej przestępczości, ale nie cyberprzestępstw. Według ekspertów niektóre kraje, głównie Rosja i Chiny, ignorują przestępczość w cyberprzestrzeni, chyba że zagraża ona ich interesom narodowym (Kshetri 2009: 141–144). Na poziomie krajowym nie ma również współpracy na linii biznes–władza polityczna. Według niektórych szacunków tylko około 10% cyberprzestępstw jest zgłaszanych na policji. Większość firm obawia się utraty swojej wiarygodności, złego PR, zniszczenia reputacji oraz spadku cen akcji. Dotyczy to głównie instytucji finansowych i firm zajmujących się gromadzeniem danych wrażliwych oraz przedsiębiorstw zajmujących się sprzedażą internetową (tamże).

Złodzieje w cyberprzestrzeni (*cyberthieves* – hakerzy, prankerzy i idealiści tworzący robaki w „słusznej" sprawie) – jak już wspomniano – z łatwością włamują się przez bramki zabezpieczające systemy informacyjne instytucji finansowych, korporacji i agencji rządowych. Dokonywanie hakerstwa stało się usługą i biznesem o ilości i jakości niespotykanej do tej pory. Jedna ze znanych grup – o nazwie LulzSec – włamała się do takich korporacji jak Bethesda Softworks i Minecraft; udało jej się wejść na poufną stronę internetową CIA, włamała się też na strony zawierające informacje o rachunkach klientów Citibank. Współcześni cyberprzestępcy skierowali swoją uwagę na portale społecznościowe. Zamiast atakować zabezpieczenia wielkich korporacji, naruszają ich tajemnice za pomocą inżynierii społecznej. Włamują się do poczty mailowej pracowników i wysyłają do nich e-maile od rzekomego przyjaciela lub kolegi. Jest to technika nazwana *spear phishing* (Nykodym, Kahle-Piasecki, Ariss, Toussaint 2010: 252–260): pomysłem jest identyfikowanie wrażliwych celów – powiedzmy kogoś w zasobach ludzkich lub finansach – i za ich pomocą przedostanie się do korporacyjnej sieci internetowej w celu kradzieży danych (biznesowych, medycznych i innych). Zupełnie nowym przestępstwem jest stosowanie w sieci tzw. *matrix bubbling up*. Jeśli haker wedrze się już do sieci społecznej, **rozprzestrzenia się** we wszystkich kierunkach, w sposób zarówno legalny, jak i nielegalny. Na dodatek hakerzy zaczęli korzystać z telefonów komórkowych na coraz szerszą skalę (Saporito 2011: 50–55).

Takie grupy hakerów jak LulzSec i Anonymous regularnie potwierdzają i udowadniają, że nasze dane przekazywane korporacjom i instytucjom nie są dostatecznie zabezpieczone. Grupy hakerów mogą włamać się do tak dobrze zabezpieczonych systemów jak: MasterCard, Amazon i PayPal. Już sama nazwa LulzSec jest grą pierwszych liter słów *laugh out loud – LOL*, a hakerzy twierdzą, że włamują się do sieci dla zabawy i śmiechu. Jej członkowie są na tyle zręczni, żeby włamać się na stronę FBI, ale jednocześnie za pomocą Twittera ostrzec przed tym, co zrobili. Kiedy jedna z firm zabezpieczających systemy komputerowe zaoferowała dziesięć tysięcy dolarów za włamanie się na jej strony, LulzSec zrobiła to

i nie przyjęła pieniędzy zgodnie ze swoją filozofią ostrzegania społeczeństwa przed tym, co niezauważalne na co dzień – hakingiem banków, przedsiębiorstw i osób prywatnych (Saporito 2011: 50–55).

Ponadto hakerzy odkryli, że małe i średnie przedsiębiorstwa są o wiele bardziej wrażliwe na ich ataki niż wielkie korporacje, ponieważ nie mogą sobie pozwolić na drogie zabezpieczenia antywirusowe. Problemem jest też Facebook – jeśli użytkownik zaprosi nieodpowiednią osobę i wejdzie na stronę rekomendowaną przez rzekomego „znajomego", może wpaść w spore kłopoty. Facebookowy robak (*bug*) zwany *Koobface* może dotrzeć do każdego konta i robi to, infekując każdego dnia wiele z nich. Hakerzy używają danych ze stron portali społecznościowych w celu tworzenia indywidualnych profili wiarygodności kredytowej. Nawet jeśli nie ma się konta na Facebooku, ktoś je może stworzyć – w takiej właśnie sytuacji znalazł się pewnego razu szef Interpolu (Saporito 2011: 50–55).

Przekrętem stulecia nazwane zostało cyberprzestępstwo w kanadyjskim Calgary, gdzie gang elektronicznych złodziei włamał się do systemu firmy obsługującej karty debetowe typu pre-paid. Przekręt polegał na zakupie kilku kart w różnych miejscach i doładowaniu każdej kwotą 15 dolarów. Hakerzy włamali się potem do systemu firmy wydającej te karty z zapisanymi limitami. Błyskawicznie podwyższyli limit każdej karty do dziesiątek tysięcy dolarów. W ciągu jednego weekendu pobrali w różnych bankach na całym świecie około miliona dolarów. Okazało się, że FIS – Fidelity National Information Service, jedna z największych firm zajmujących się obsługą technologii bankowych kart płatniczych na całym świecie, dla której bezpieczeństwo jest jednym z najważniejszych priorytetów, padła ofiarą dokładnie takiego samego przekrętu jak firma w Calgary. Straciła jednak nie milion, ale 13 mln dolarów za pomocą 22 zmanipulowanych kart (Glenny 2011: 33–35).

Jedna z najnowszych metod przestępczych opiera się na *scareware*, czyli złośliwym oprogramowaniu, i została doprowadzona do perfekcji przez ukraińską firmę sprzedającą programy antywirusowe Innovative Marketing (IM). Jednak kliknięcie określonego linku na stronie powodowało, że użytkownik dostawał ostrzeżenie, że jego komputer jest zarażony i jedynym sposobem miało być kliknięcie w niżej wskazany link i zakup Malaware Destroyer 2009 albo inny produkt IM. Po zapłaceniu 40 euro pojawiała się instrukcja, jak usunąć wirusa. Przekręt polegał na tym, że nowy program wcale nie chronił przed wirusami ani ich nie usuwał. Współcześni hakerzy nauczyli się korzystać z outsourcingu. Cyberprzestępcy nowej generacji kontrolują olbrzymią liczbę komputerów-zombi. Haker może wypożyczyć je innym hakerom, którzy wykorzystują je potem do łamania zabezpieczeń banków i instytucji finansowych, wysyłania setek wiadomości przeciążających serwery, wyszukiwania numerów, danych do logowania i informacji finansowych (numery kart kredytowych). Na wykradzione w internecie pieniądze również znalazła się metoda outsourcingu, która polega na wykorzystaniu *money mules* – mułów pieniężnych. Pod przykrywką

legalnej działalności przestępcy oferują ludziom-mułom pewną sumę pieniędzy za pracę na domowym komputerze. Muły korzystają z legalnych kont w imieniu swoich pracodawców. Na przykład otrzymują 200 dolarów i przesyłają 180 do cyberprzestępcy, zatrzymując 20 dla siebie (Glenny 2011: 33–35).

W przypadku procederu prania pieniędzy e-przestępcy wykorzystują rozwój nowych technologii i piorą je za pomocą elektronicznych instrumentów płatniczych, korzystania z wirtualnych kasyn i gier oraz aukcji internetowych. Wirtualny świat Internetu i nowych technologii pozwala na nielegalne przetwarzanie danych i ukrywanie przychodów nielegalnego pochodzenia. Proces prania pieniędzy tradycyjnie polega na wprowadzeniu nielegalnych pieniędzy w system finansowy w celu uniknięcia ich konfiskaty. Można to zrobić przez wpłacanie na konto gotówki poniżej minimalnego progu raportowania, co czyni je trudnymi do monitorowania. W ten sposób tworzą się kanały, przez które brudne pieniądze zaczynają przepływać przez różne konta w celu ukrycia ich źródeł pochodzenia. Następnie e-przestępcy podejmują gotówkę umieszczoną w różnych instrumentach finansowych i za pomocą Internetu inwestują w zakup nieruchomości, cennych przedmiotów, kamieni szlachetnych i dzieł sztuki. Do najbardziej znanych technik elektronicznych systemów płatności należą przelewy przy użyciu fałszywej tożsamości na zakup akcji i obligacji oraz złota. W przypadku wirtualnych kasyn, aby uzyskać dostęp do wirtualnej gry, należy stworzyć konto na stronie internetowej, pobrać oprogramowanie i korzystać z karty kredytowej lub pobierać pieniądze z elektronicznego funduszu na pokrycie przegranych sum lub wpłaty wygranych kwot. W ten sposób można uzasadnić pochodzenie pieniędzy z wygranej gry. Z kolei na aukcjach internetowych przestępcy mogą podbijać cenę przedmiotu, a sprzedający – również zaangażowany w proceder – otrzymuje w ten sposób znaczną sumę pieniędzy o charakterze legalnym. Powstanie gier wirtualnych, takich jak Entropia Universe i Second Life, stwarza nowe możliwości prania pieniędzy. Gracze mogą sprzedawać wirtualne produkty w realnym świecie za prawdziwe pieniądze, które potem wycofane z wirtualnego konta uznane są za legalne, a ich źródło nie jest zidentyfikowane (Glenny 2011: 33–35).

Eksperci amerykańscy oszacowali, że w 2009 r. straty spowodowane przez cyberprzestępczość i wywiad przemysłowy wyniosły w samych Stanach Zjednoczonych około 1 biliona dolarów, ale są to jedynie dane szacunkowe, będące wynikiem jakichś algorytmów lub wymyślone, jak niektórzy uważają, przez firmy sprzedające zabezpieczenia w celu nakręcenia i zwiększenia sprzedaży programów antywirusowych (Glenny 2011: 33–35).

Rodzaje i formy działalności cyberprzestępczej bardzo szybko się zmieniają. Jeszcze do niedawna centrum systemu przestępczego były tzw. **strony *carderów***, np. CarderPlanet, Shadowcrew i DarkMArket. Najbardziej znaną stroną była CarderPlanet, która działała na serwerze z Odessy. Wtajemniczone osoby mogły kupować i sprzedawać skradzione numery kart kredytowych oraz złośliwe oprogramowania (wirusy, trojany

i robaki) do infekowania komputerów. Można też było tam znaleźć instrukcje obsługi najnowszych oprogramowań do łamania zabezpieczeń albo wynająć *botnet* – czyli sieć tysięcy zainfekowanych komputerów-zombi do ataku na wybrany cel. CarderPlanet była kamieniem milowym w historii cyberprzestępczości, ponieważ jej twórcy wprowadzili do użycia system rachunków zastrzeżonych (typu *Escrow*). Dzięki temu cyberprzestępcy rozwiązali podstawowy problem: jak handlować i współpracować przez Internet z kimś, kto łamie prawo, a więc komu nie można zaufać. Początkowo cyberprzestępcy działali pojedynczo i nie łączyli się w grupy. Ostatnio jednak zaczęli łączyć się wokół charyzmatycznych hakerów, a strony *carderów*, jak CarderPlanet, wypadły z obiegu, bo były zbyt łatwo infiltrowane przez stróżów prawa. Obecne grupy cyberzłodziei przypominają tradycyjnie zorganizowaną przestępczość, ponieważ jest w nich jasna hierarchia i podział pracy (Glenny 2011: 33–35).

Podsumowując: współczesny świat charakteryzuje się wielowymiarowością, chaotycznością oraz złożonością zjawisk i procesów. Jest pełen ryzyk i zagrożeń, a jednym z nich jest przestępczość zorganizowana, związana w dużej mierze ze sferą gospodarki nieoficjalnej (nieformalnej, szarej, nielegalnej). Podwójna **wirtualność** gospodarki nieoficjalnej wynika z faktu, że oficjalnie jej nie ma (nie jest rejestrowana, nie podlega kontroli organów państwa czy organizacji międzynarodowych, nie jest uwzględniana w PKB). Druga **wirtualność** związana jest z przenoszeniem działań przestępczości zorganizowanej za pomocą najnowszej technologii informatycznej do cyberprzestrzeni.

BIBLIOGRAFIA

1. Chomsky N. (2000) Marginalizing the Masses. *Journal of International Affair*, 53, 2, s. 723–737.
2. Choo K.-K.R. (2008) Organised crime groups in cyberspace: a typology. *Trends in Organized Crime*, 11, 3
3. Ćwikowski D. (2012) Gospodarka nieoficjalna a system bezpieczeństwa ekonomicznego państw. W: K. Raczkowski (red.), *Bezpieczeństwo ekonomiczne. Wyzwania dla zarządzania państwem*. Warszawa: Wolters Kluwer.
4. Feige E.L. (red.) (1989) *The Underground Economies. Tax Evasion and Information Distortion*. Cambridge: Cambridge University Press.
5. Fleming M.H., Roman J., Farrell G. (2000) The Shadow Economy. *Journal of International Affairs*, 53, 2.
6. Frey B., Scahneider F. (2001) Informal and Underground Economies. W: N. Smelser, P. Baltes (red.), *International Encyclopedia of the Social and Behavioral Sciences*. London: Elsevier Science Ltd.
7. Gikas G. (1992) Przyczyny i konsekwencje gospodarki drugiego obiegu. *Gospodarka Narodowa*, 9.

8. Gilmore W.C. (1999) *Brudne pieniądze. Metody przeciwdziałania praniu pieniędzy*. Warszawa: PWE.
9. Glenny M. (2011) Hack im w smak. *Forum*, 46, 14–21.11.2011, s. 33–35.
10. Goglio S. (2004) Crime, Collective Action and Development. *European Planning Studies*, 12, 6, s. 853–865.
11. Goławska M. (2002) Piracki proceder. *Marketing i rynek*, 1, s. 36–40.
12. Hołyst B. (1997) *Kryminologia*, Warszawa: Wydawnictwa Prawnicze PWN.
13. Jakubski K.J. (2006) Bezpieczna karta? W: J. Kosiński (red.), *Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych*. Szczytno: Wydawnictwo Wyższej Szkoły Policyjnej w Szczytnie.
14. Jarociński W. (1995) Przegląd metod szacunku rozmiarów szarej gospodarki. W: *Szara strefa gospodarki. Wybrane problemy*. Studia i prace Zakładu Badań Statystyczno-Ekonomicznych. Warszawa: ZBSE, s. 49–66.
15. Jasiński W. (2001) *Przeciw szarej strefie. Nowe zasady zapobiegania praniu pieniędzy*. Warszawa: Poltext.
16. Johnson S., Kaufman D., Zoida-Lobaton P. (1998) Regulatory Discretion and the Unofficial Economy. *The American Economic Review*, 88, 2, s. 387–392.
17. Kozłowski P. (2004) *Gospodarka nieformalna w Polsce. Dynamika i funkcje instytucji*. Warszawa: Instytut Badań Ekonomicznych PAN.
18. Krajewska A. (2004) *Podatki – Unia Europejska, Polska, kraje bałtyckie*. Warszawa: PWE.
19. Kshetri N. (2009) Positive Externality, Increasing Returns, and the Rise in Cybercrimes. *Communications of the ACM*, 52, 12, s. 141–144.
20. Laskowska K. (2011) Przestępczość gospodarcza. W: E.W. Pływaczewski (red.), *Przestępczość zorganizowana*. Warszawa: C.H. Beck.
21. Mróz B. (2002) *Gospodarka nieoficjalna w systemie ekonomicznym*. Warszawa: Oficyna Wydawnicza SGH.
22. Nykodym N., Kahle-Piasecki L., Ariss S., Toussaint T.A. (2010) Cybercrime and Business: How to not Get Caught by the Online Phisherman. *Journal of International Commercial Law and Technology*, 5, 4, s. 252–260.
23. Obława na harcowników (2001). *Forum*, 17–30.12.2001, s. 36.
24. Rajewski Z., Zienkowski L. (1994) *Szara strefa w systemie rachunków narodowych*. Warszawa.
25. Saporito B. (2011) Hack Attack. *Time*, 7/4, 178, 1, s. 50–55.
26. Schneider F. (2005) The Size of Shadow Economies in 145 Countries from 1999 to 2003. *Brown Journal of World Affair*, 11, s. 113–129.
27. Schneider F., Enste D.H. (2000) Shadow Economies: Size, Causes, and Consequences. *Journal of Economic Literature*, 38, s. 20–25.
28. Shinder D.L.(2004) *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*. Gliwice: Helion.
29. Ştefan I. (2011) Cyber Crime. *Juridical Current*, 14, 3.

30. Szwarc J. (2009) Prawne aspekty przestępczości teleinformatycznej. W: J. Bednarek, A. Andrzejewska (red.), *Cyberświat – możliwości i zagrożenia*. Warszawa: Wydawnictwo Akademickie „Żak" Teresa i Józef Śniecińscy.
31. Wójcik W. (2001) *Kryminologiczna ocena transakcji w procesie prania pieniędzy*. Warszawa: Twigger.
32. Wysocki W. (2003) *Przemyt a bezpieczeństwo ekonomiczne Polski*. Warszawa: Ulmak.