

**Marcin GÓRNIKIEWICZ**  
Wyższa Szkoła Bezpieczeństwa

## **OCHRONA WŁASNOŚCI INTELEKTUALNEJ W ROZUMIENIU WIPO JAKO ELEMENT BEZPIECZEŃSTWA GOSPODARCZEGO PAŃSTWA**

*Dobry gospodarz nie myśli o kopaniu studni, gdy się pali. Myśli o tym znacznie wcześniej. Problem, o którym mowa, wymaga podejmowania działań z dużym wyprzedzeniem w celu zabezpieczenia się przed tym zjawiskiem i jego następstwami.<sup>1</sup>*

Bezpieczeństwo gospodarcze to jeden z sektorów wchodzących w zakres systemu bezpieczeństwa wewnętrznego państwa. W ramach tegoż sektora mieszczą się również prywatne podmioty gospodarcze. Stanowią one jeden z najczulszych punktów podsystemu bezpieczeństwa gospodarczego. Powodem takiego stanu rzeczy jest ich nierozzerwalna łączność z zewnętrznymi czynnikami ekonomicznymi i możliwość wywierania przez nie wpływu na państwo ich pochodzenia nie tylko, przez inne państwa, ale również prywatne podmioty gospodarcze o międzynarodowym zasięgu oddziaływania (np. korporacje). Działania takie mogą mieć następujące konsekwencje dla gospodarki krajowej: zmniejszenia podaży walut obcych; przerwania dopływu kapitału z zagranicy; ograniczenia lub likwidacji płynności finansowej; wywołanie wzrostu zadłużenia zagranicznego; wywołanie spadku wartości waluty. Odrębnym działaniem, ale nie mniej istotnym z punktu widzenia gospodarczego interesu państwa jest kradzież własności intelektualnej prywatnych podmiotów gospodarczych. W moim przekonaniu nie jest możliwe właściwie funkcjonowanie gospodarki każdego państwa, jeśli nie funkcjonują skuteczne mechanizmy ochrony nie tylko podmiotów publicznych, ale również prywatnych. Idąc krok dalej, można powiedzieć, iż w interesie społeczeństwa jest, aby państwo narzuciło odgórnie pewne normy bezpieczeństwa na podmioty prywatne w zakresie wszelkich spraw ich dotyczących – przy założeniu, że podmioty te nie są w stanie same o to zadbać.

John Naisbitt już na początku lat 80 XX wieku stwierdził: „Obecnie produkujemy informację tak jak niegdyś masowo produkowaliśmy samochody”.<sup>2</sup> To krótkie zdanie najdobitniej oddaje znaczenie i realną wartość jakiej nabrała informacja, stając się tym samym towarem, a więc dobrem, o które warto się troszczyć na równi z każdym innym czynnikiem przedsiębiorstwa. Praktycznym odzwierciedleniem powyższego stwierdzenia są słowa wypowiedziane przez P. F. Drucker opisujące znaczenie informacji dla społeczeństwa japońskiego: „Japonia w latach czterdziestych radziła sobie bardzo dobrze zarówno z tradycyjną produkcją, jak i nowoczesną, opierającą się na najnowszych osiągnięciach wiedzy. Ale błyskawiczny rozwój Japonii nie nastąpił przez „tworzenie” wiedzy. Jeśli idzie o technologię i zarządzanie większość japońskiej wiedzy została stworzona gdzie indziej, głównie w Stanach Zjednoczonych”.<sup>3</sup> Nota bene podobny schemat działania miał i nadal ma miejsce we współczesnych Chinach, gdzie obok fabryk stawianych przez producentów znanych na świecie marek powstają identyczne fabryczki ko-

<sup>1</sup> E. Frejtag-Mika; Z. Kołodziejak; W. Putkiewicz: *Bezpieczeństwo ekonomiczne we współczesnym świecie*. Radom 1996, s. 28

<sup>2</sup> P. Bączek: *Zagrożenia informacyjne, a bezpieczeństwo państwa polskiego*. Toruń 2005, s. 47

<sup>3</sup> Ibidem, s. 48

piujące proces produkcji tych pierwszych. Paradoksalnie stworzono zagranicznym inwestorom doskonałe warunki dla lokalizacji ich produkcji, nie tylko po to, aby ściągnąć do Chin część ich kapitału, ale po prostu po to, aby bez większego trudu kopiować ich technologię. Innym przykładem tej mentalności są współczesne Włochy, a konkretnie okolice Neapolu. R. Saviano opisuje przekupienie przez chińskiego przedsiębiorcę doskonałego specjalisty fachu krawieckiego. Mężczyzna ten, na co dzień pracujący w jednym z licznych w tym rejonie, nielegalnych zakładów zgadza się na ofertę złożoną mu przez Chińczyka. Dotyczy ona, nie podkupienia jego osoby, ale zapłaty za udzielenie lekcji krawiectwa na najwyższym poziomie dla chińskich pracowników. Dzięki temu jego cichy zleceniodawca uzyskuje możliwość złożenia swojej oferty na podziemnym rynku usług krawieckich dla włoskich domów mody.<sup>4</sup> Azjata zapłacił za wiedzę, a więc informację mając świadomość, iż jest ona dużo cenniejsza niż zatrudnienie jednego lub kilku specjalistów, którzy tę wiedzę zachowaliby dla siebie. Na tym właśnie polega potężny potencjał związany z własnością intelektualną w gospodarce.

Wracając do samego pojęcia „własności intelektualnej” można się odnieść do definicji uznawanej przez Światową Organizację Własności Intelektualnej – jedną z wyspecjalizowanych organizacji przy ONZ (ang. *World Intellectual Property Organization*, skrót *WIPO*). Zgodnie z definicją zawartą w dokumencie wydanym przez WIPO własność intelektualna to szeroko rozumiany proces twórczy ludzkiego umysłu. Prawa chroniące własność intelektualną mają na celu zabezpieczyć interes twórców uposażając ich w prawo własności do ich pomysłów.<sup>5</sup> Konwencja założycielska WIPO z 1967 roku wymienia następujące kategorie własności intelektualnej chronionej przez prawo:

- prace literackie, artystyczne i naukowe;
- przedstawienia sceniczne, fonogramy, audycje;
- innowacje we wszystkich obszarach ludzkiej aktywności;
- odkrycia naukowe;
- wzory przemysłowe;
- znaki towarowe, nazwy i oznaczenia usług;
- wszelkie inne rezultaty intelektualnej aktywności w przemyśle, nauce, obszarach artystycznych i naukowych.

Własność intelektualną dzieli się na dwa rodzaje: własność przemysłową i prawa autorskie. Własność przemysłowa to patenty chroniące innowacje przemysłowe, wzory przemysłowe, znaki towarowe, nazwy i oznaczenia usług przed nieuczciwą konkurencją. Prawa autorskie to wytwory artystyczne np. książki, utwory muzyczne, dzieła malarskie, filmy, technologiczne takie jak programy komputerowe czy elektroniczne bazy danych. W tym rozumieniu w kategorii własności intelektualnej będą się również mieścić wszelkie autorskie projekty danej firmy związane z nowymi ideami jej rozwoju, z układaniem strategii jej ekspansji na konkretnych rynkach, nowe rozwiązania mające usprawnić wewnętrzną organizację w danej firmie itp. WIPO ściśle współpracuje ze Światową Organizacją Handlu (*WTO*). Owoce tej współpracy jest np. porozumienie *TRIPS* dotyczące handlowych aspektów praw własności intelektualnej oraz ich ochrony, dochodzenia i egzekwowania. Porozumienie to reguluje wszystkie obszary własności intelektualnej,

<sup>4</sup> R. Saviano: *Gomorra, Podróż po imperium kamorry*. „Czytelnik”. Warszawa 2008, s. 25-48

<sup>5</sup> Understanding Copyright And Related Rights. World Intellectual Protection Organization. Genewa, s. 3-6

tj. ochronę dla praw autorskich i pokrewnych, w tym ochronę *programów komputerowych*, *baz danych* oraz ochronę wykonawców, producentów, nagrań dźwiękowych, organizacji nadawczych, patentów, praw do wzorów przemysłowych, *znaków towarowych*, geograficznych oznaczeń pochodzenia towarów, a także ochronę poufnego tzw. *know-how* oraz kontrolę praktyk antykonkurencyjnych w licencjach umownych.

W Polsce zagadnienie własności intelektualnej zostało uregulowane przez Ustawę z dnia 30 czerwca 2000 r. *Prawo własności przemysłowej*; Ustawę z dnia 4 lutego 1994 r. *o prawie autorskim i prawach pokrewnych*; Ustawę z dnia 27 lipca 2001 r. o ochronie baz danych i Ustawę z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji. Zgodnie z Ustawą o prawie autorskim i prawach pokrewnych – prawo autorskie obejmuje swoją ochroną każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia (utwór).<sup>6</sup> W szczególności przedmiotem prawa autorskiego są utwory:<sup>7</sup> wyrażone słowem, symbolami matematycznymi, znakami graficznymi (literackie, publicystyczne, naukowe, kartograficzne oraz programy komputerowe); plastyczne; fotograficzne; lutnicze; wzornictwa przemysłowego; architektoniczne, architektoniczno-urbanistyczne i urbanistyczne; muzyczne i słowno-muzyczne; sceniczne, sceniczno-muzyczne, choreograficzne i pantomimiczne; audiowizualne (w tym filmowe).

Natomiast z ochrony polskiego prawa nie korzystają już odkrycia, idee, procedury, metody i zasady działania oraz koncepcje matematyczne - Ochroną objęty może być wyłącznie sposób wyrażenia.<sup>8</sup> Według Ustawy Prawo własności przemysłowej, która w sposób pośredni odnosi się do definicji pojęcia własności przemysłowej poprzez wyodrębnienie enumeratywnego katalogu stosunków objętych jej działaniem normuje: stosunki w zakresie wynalazków, wzorów użytkowych, wzorów przemysłowych, znaków towarowych, oznaczeń geograficznych i topografii układów scalonych.<sup>9</sup>

Celem przedstawionych powyżej definicji prawnych własności intelektualnej na poziomie globalnym i krajowym jest jedynie przybliżenie treści samego pojęcia. W dalszej części niniejszego opracowania posłużę się szerszą definicją reprezentowaną przez WIPO z dwóch powodów. Po pierwsze temat pracy odnosi się do gospodarki państwa, ale w odniesieniu do gospodarki światowej, bez łączności z którą żadne państwo na świecie nie byłoby w stanie właściwie funkcjonować. Po drugie celem pracy jest zobrazowanie jakie może mieć skutki dla gospodarki państwa niewłaściwe zabezpieczenie wszelkich informacji istotnych dla danej firmy – na poziomie poszczególnych przedsiębiorstw – a nie rozwijanie zagadnienia różnic interpretacyjnych pojęcia „własność intelektualna”.

Wartość określonej „własności intelektualnej” dla potencjalnego agresora będzie zależeć od samej treści danej własności (np. dokumentacja nowego urządzenia, które może zrewolucjonizować określoną gałąź przemysłu) oraz od pozycji podmiotu, który wytworzył lub przechowuje tę własność, na rynku globalnym lub lokalnym (np. tajny biznesplan, badania rynku pod określony profil działalności, plan agresywnego przejęcia innych firm etc.). Posiadając dostęp do informacji wie-

<sup>6</sup> Prawo autorskie, art. 1 ust. 1

<sup>7</sup> Prawo autorskie, art. 1 ust. 2

<sup>8</sup> Prawo autorskie, art. 2prım

<sup>9</sup> Prawo o własności przemysłowej, art. 1 ust. 1 pkt. 1

lu podmiotów gospodarczych, można wywołując odpowiednie zdarzenia na rynku ukierunkowywać działalność części prywatnego sektora gospodarczego. Dzięki temu podmiot zewnętrzny posiadający taką wiedzę, może de facto regulować sytuację na rynku danego państwa – co również oznacza, że w stosownym dla siebie momencie może doprowadzić do wybuchu kryzysu gospodarczego. Przykładowo jeśli podmiot zewnętrzny X dowiedział się o perspektywach rozwoju kluczowych dla gospodarki danego państwa firm X, Y, Z, może wywołując rozmaite zdarzenia wpasowujące się w strategię ekspansji lub obrony tychże firm nakierować je na działanie w wytyczonych przez siebie kierunkach. Podmiot zewnętrzny X ma 90% pewności, że firmy X, Y, Z zachowają się w określony sposób, dlatego że warunki które wywołał zostały przewidziane w ich planach. Idąc dalej nowe zachowanie się firm X, Y, Z wywołało określone skutki w stosunku do MSP<sup>10</sup> w danym państwie. Natomiast podmiot zewnętrzny X tworząc daną sytuację oczywiście odgórnie przewidział, że określone zachowanie się firm X, Y, Z wpłynie na ceny kursów akcji tychże firm oraz na ceny określonych produktów. Wiedząc o tym podmiot zewnętrzny mógłby w krótkim czasie zarobić pokaźną sumę pieniędzy. To jednak nie koniec – podmiot zewnętrzny X może również chcieć doprowadzić do sytuacji kryzysowej w gospodarce danego państwa i wówczas na bazie posiadanych informacji stworzy wieloetapowy plan działania, który skończy się upadłością wielu podmiotów z prywatnego sektora gospodarczego lub koniecznością zadłużenia się u podmiotów zewnętrznych – nierzadko, uprzednio wyselekcjonowanych przez podmiot X. Wówczas takie działania uderzają bezpośrednio w sektor bezpieczeństwa gospodarczego, będącego jednym z fundamentów systemu bezpieczeństwa wewnętrznego państwa. Reasumując już sama możliwość przyszłościowego zdobycia tak cennych informacji przez podmioty zewnętrzne – w wyniku braku skutecznych mechanizmów ochronnych szeroko pojętej własności intelektualnej w prywatnych firmach – stwarza uwarunkowania mogące doprowadzić w przyszłości do zagrożenia stabilności podsektora gospodarczego państwa. Przykładem z życia jest podniesienie przez Arabię Saudyjską ceny z baryłkę ropy z 1,90 USD na 34 USD w 1982 roku. Dla importerów oznaczało to znaczny wzrost obciążeń. Efektem powstałego wzrostu cen były właśnie spekulacje stopą procentową oraz kursem walutowym. Kolejnym skutkiem była niewypłacalność Meksyku, Brazylii i Argentyny, które ogłosiły brak możliwości do spłacania odsetek od zaciągniętych kredytów.<sup>11</sup>

Najlepszym przykładem na potencjał i zarazem siłę rażenia bronią jaką stanowi dostęp do własności intelektualnej wszelkich podmiotów gospodarczych jest raport firmy McAfee przedstawiający wyniki pierwszego globalnego badania aspektów bezpieczeństwa gospodarek opartych na informacji – „Unsecured Economies: Protecting Vital Information” (tł. „Niebezpieczne Gospodarki. Ochrona kluczowych informacji”. Z raportu wynika, że globalna recesja w bezprecedensowy sposób zwiększa zagrożenie najważniejszych informacji. Badacze z Centrum Edukacji i Badań Wiarygodności i Bezpieczeństwa Informacji Uniwersytetu Purdue przeprowadzili badanie ankietowe ponad 800 szefów informatyki z USA, Wielkiej Brytanii, Niemiec, Japonii, Chin, Indii, Brazylii i Dubaju. W wyniku badań ustalono źródła najważniejszych informacji takich, jak własność intelektualna, miejsca ich przecho-

<sup>10</sup> MSP – Małe i Średnie Przedsiębiorstwa

<sup>11</sup> A. Bień: *Kryzys zadłużenia*. Warszawa 1992, s. 18-22

wywania, sposób przesyłania oraz okoliczności utraty. Zgodnie z oceną badanych firm tylko w minionym roku łączne straty związane z utratą własności intelektualnej sięgnęły 4,6 miliarda dolarów, natomiast wydatki na likwidację skutków naruszenia bezpieczeństwa sięgnęły 600 milionów dolarów. W oparciu o te wyniki, twórca raportu – McAfee szacuje, że w skali globalnej straty firm z tego tytułu przekroczyły bilion dolarów.

Raport „Niebezpieczne gospodarki” przedstawiony przez McAfee wskazuje, że w takich krajach, jak Chiny, Brazylia, czy Japonia kluczem do bezpieczeństwa danych jest możliwość ich bezpiecznego przechowywania. Sześćdziesiąt procent respondentów z Chin deklaruje, że właśnie względy bezpieczeństwa skłoniły ich do przechowywania kluczowych informacji poza granicami kraju. Według McAfee Polska - Polska i inne kraje Europy Środkowej stały się ważnym zapleczem outsourcingowym dla międzynarodowych koncernów zarówno w obszarze produkcji, jak i przetwarzania danych. Polskie przedsiębiorstwa mają dostęp do poufnych informacji firm niemieckich, amerykańskich, brytyjskich, a nawet chińskich i japońskich. Zarazem McAfee Polska zaznacza że, aby utrzymać tę pozycję koniecznością będzie stworzenie i utrzymania przez polskie firmy systemów bezpieczeństwa spełniających najwyższe standardy.<sup>12</sup> Wnioski płynące z raportu są następujące:<sup>13</sup>

1) Recesja zwiększa zagrożenie własności intelektualnej.

Z raportu wynika, że globalny kryzys finansowy i jego wpływ na bezpieczeństwo kluczowych danych takich, jak własność intelektualna według 39% respondentów jest zagrożona w dużo większym stopniu, niż dotychczas.

2) Zróżnicowane zaangażowanie w ochronę kluczowych informacji.

Podmioty z krajów rozwijających się przykładają większą wagę do ochronę własności intelektualnej i inwestują w nią więcej, niż podobne firmy zachodnie. W Brazylii, Chinach i Indiach wydaje się na bezpieczeństwo więcej, niż w Niemczech, Wielkiej Brytanii, USA czy Japonii. Siedemdziesiąt cztery procent respondentów z Chin i sześćdziesiąt osiem procent respondentów z Indii dokonało inwestycji w bezpieczeństwo własności intelektualnej w celu zwiększenia konkurencyjności.

3) Własność intelektualna stanowi obecnie rodzaj międzynarodowej waluty.

Własność intelektualna staje się nowym celem cyberprzestępców. Eksperci twierdzą, że odnotowano wzrost liczby przypadków naruszenia bezpieczeństwa danych korporacyjnych przez zorganizowane grupy przestępcze. Cyberprzestępcy coraz częściej wykorzystują zaawansowane techniki phishingu do ataku na członków zarządów przedsiębiorstw. Trzydzieści dziewięć procent respondentów za najważniejsze zadanie uznaje ochronę własności intelektualnej przed próbami jej wykradzenia.

4) Pracownicy kradną własność intelektualną dla pieniędzy oraz by zyskać przewagę na rynku pracy.

<sup>12</sup> Bankier.pl – Polski Portal Finansowy, 10.02.2009, Firmy straciły bilion dolarów na skutek kradzieży własności intelektualnej – [http://www.bankier.pl/wiadomosci/print.html?article\\_id=1905756](http://www.bankier.pl/wiadomosci/print.html?article_id=1905756)

<sup>13</sup> Informacje o badaniu – Globalne badanie zostało przeprowadzone przez Centrum Edukacji i Badań Wiarygodności i Bezpieczeństwa Informacji (CERIAS - Center for Education and Research in Information Assurance and Security) Uniwersytetu Purdue za pomocą ankiety i objęło 800 szefów informatyki z USA, Wielkiej Brytanii, Niemiec, Japonii, Chin, Indii, Brazylii i Dubaju

Rośnie liczba pracowników, którzy mając problemy finansowe decydują się na kradzież kluczowych danych przedsiębiorstwa. W warunkach globalnej recesji, wobec groźby utraty pracy i malejącej możliwości normalnego zatrudnienia „cybernetyczne krety” wykradają dane, które mogą być atrakcyjne dla przyszłych pracodawców, by zwiększyć swą wartość na rynku pracy. Według czterdziestu dwóch procent respondentów, zwalniani pracownicy stanowią największe zagrożenie dla kluczowych informacji.

5) Bezpieczeństwo własności intelektualnej, a geografia.

Uwarunkowania geopolityczne mają wpływ na percepcję kwestii bezpieczeństwa informacji. Badane firmy uznały Chiny, Pakistan i Rosję za strefy podwyższonego ryzyka z licznych powodów o naturze prawnej, kulturowej i gospodarczej. Z tego powodu dwadzieścia sześć procent respondentów unika przechowywania swej własności intelektualnej w Chinach. Zarazem aż czterdzieści siedem procent respondentów z Chin uważa, że największe zagrożenie dla ich własności intelektualnej stanowią Stany Zjednoczone.

6) Zagrożenia i metody obrony przed zagrożeniami.

P. Bączek, idąc za myślą R. Czechowskiego i P. Sienkiewicza wskazuje: „Współczesne społeczeństwa potrzebują coraz więcej informacji, wraz z rozwojem cywilizacji, techniki, rośnie dążenie do zdobywania i gromadzenia wiadomości o otoczeniu zewnętrznym i wewnętrznym.<sup>14</sup> Słowa te można idealnie odnieść do sytuacji przedsiębiorstwa, które nie posiada efektywnego systemu gromadzenia i przechowywania wiedzy. Wyciekające informacje mogą się bardzo przyczynić do jego upadku.

Podmioty zewnętrzne mogą wykorzystywać rozmaite metody nielegalnego pozyskiwania cennych informacji. Można wyróżnić następujące katalogi takich metod: cyberprzestępczość oraz wywiad gospodarczy. Cyberprzestępczość są to wszelkie operacje dokonywane za pośrednictwem Internetu, polegające na łamaniu prawa i obowiązujących norm celem wywołania określonego efektu lub celem osiągnięcia określonych korzyści. Z kolei wywiad gospodarczy można podzielić na dwie kategorii czyli tzw. biały wywiad przeprowadzany zgodnie z prawem i panującymi w danym społeczeństwie normami oraz wywiad przeprowadzany w sprzeczności z tymi normami oraz prawem dla uproszczenia określony jako tzw. czarny wywiad.

7) Cyberprzestępczość.

Obecnie obok tradycyjnych metod nielegalnego pozyskiwania informacji tzw. czarny wywiad – funkcjonują metody związane z atakami na wewnętrzne sieci informatyczne w danych podmiotach gospodarczych. Zgodnie ze słowami jednego z funkcjonariuszy odpowiedzialnych za ochronę łączności w ramach jednej z instytucji bezpieczeństwa publicznego nie ma obecnie praktycznej możliwości zabezpieczenia się przed każdym rodzajem włamania przez łączę sieciowe.<sup>15</sup> Najpewniejszym zabezpieczeniem jest odłączenie dostępu do sieci zewnętrznych – czyli Internetu. Wówczas jedyną możliwą metodą nieuprawnionej ingerencji pozostaje mechaniczne podłączenie się do sieci wewnętrznej. Rodzajem cyberagresji, która mieści się w tematycznych ramach niniejszego opracowania jest każda, której celem jest pozyskanie określonych informacji – a ściślej uzyskaniem dostępu do wła-

<sup>14</sup> P. Bączek: *Zagrożenia informacyjne, a bezpieczeństwo państwa polskiego*. Toruń 2005, s. 48

<sup>15</sup> Źródło własne

sności intelektualnej danego podmiotu. Podłączenie się do sieci wewnętrznej danej firmy lub tylko do pojedynczych jednostek daje dostęp nie tylko do zasobów przechowywanych na danej jednostce, ale również możliwość włamania się na pocztę elektroniczną, na komunikatory internetowe jak GG, Skype, uzyskanie dostępu do haseł i numerów kont bankowych i kart kredytowych używanych przez pracowników firmy, lub upoważnione osoby w imieniu firmy. Potencjalne możliwości wynikające z uzyskania takiego dostępu do informacji, a wręcz podjęciu działań mających na celu dyskredytowanie danej firmy w oczach klientów lub wywołaniem niezdrowej atmosfery wśród pracowników, czy też poprzez wpływ na konta bankowe wywołaniu negatywnych konsekwencji finansowych są właściwie nieograniczone. Nasuwa się konkluzja, iż dla dobra nie tylko firmy, ale dla dobra samych pracowników powinni oni korzystać z jednostek firmowych tylko w sprawach służbowych.

#### Przestępstwa komputerowe

Trudno sobie dzisiaj wyobrazić, aby firma posiadała komputery bez dostępu do Internetu. Niestety konieczność bycia podłączonym do sieci zewnętrznych stwarza zagrożenie dla bezpieczeństwa informacji przechowywanych na tych komputerach. Można wyróżnić następujące zagrożenia<sup>16</sup>:

- Sabotaż – świadoma ingerencja w systemy komputerowe firmy mające na celu destrukcję informatyczną;
- Zagrożenia nieumyślne – powstają na skutek braku doinformowania użytkowników komputerów o możliwych zagrożeniach lub braku wyobraźni z ich strony;
- Infiltracja – przeniknięcie do różnych elementów systemu informatycznego, z wyszczególnieniem „infiltracji biernej” polegającej na śledzeniu informacji w określonym punkcie jej obiegu<sup>17</sup> oraz „infiltracji czynnej” polegającej na świadomym uzyskaniu dostępu do systemu w celu ingerencji w najbardziej wrażliwe oraz najważniejsze elementy systemu.<sup>18</sup>

Przestępstwa komputerowe można podzielić na dwie kategorie: bezpośrednie i pośrednie. W przypadku pierwszej kategorii celem działania jest kradzież z atakowanej jednostki komputerowej: oprogramowania, myśli technicznej, sprzętu, czasu pracy komputera, informacji oraz sabotaż sprzętowo-programowy. Druga kategoria natomiast dotyczy przypadku ataku na daną jednostkę celem wykorzystania jej w: oszustwie komputerowym, wykorzystaniu informacji, symulacji i planowaniu działań przestępczych przy użyciu komputera, posługiwaniu się komputerem jako środkiem komunikacji w innych działaniach przestępczych, tworzeniu systemów informatycznych na użytek działań lub organizacji przestępczych.

Wywiad gospodarczy (biały i czarny).

<sup>16</sup> P. Bączek: *Zagrożenia informacyjne, a bezpieczeństwo państwa polskiego*. Toruń 2005, s. 122-124

<sup>17</sup> W ramach infiltracji biernej możemy wyróżnić: przechwytywanie elektromagnetyczne polegające bądź na uzyskaniu dostępu do połączeń między komputerami, a terminalami, bądź do kierunkowej emisji promieniowania i na analizie sygnału odbitego od promieniującego urządzenia; podłączenie się do linii transmisji danych w sieciach telekomunikacyjnych lub przechwytywanie sygnałów drogą radiową; badanie i kopiowanie nie zabezpieczonych programów i plików; analiza makulatury lub pozostałości po nośnikach informacji pozostawionej w skutek niewłaściwej gospodarki makulaturą i brakiem demagnetyzacji nośników informacji

<sup>18</sup> W ramach infiltracji czynnej wyróżniamy: łamanie zabezpieczeń celem dostępu do dowolnego miejsca systemu informatycznego, ingerowanie w struktury systemów operacyjnych; podszywanie się pod uprawnionego użytkownika systemów komputerowych, stosowanie programów i procedur dodatkowych umieszczanych w trakcie tworzenia oprogramowania

Biały wywiad gospodarczy – charakteryzuje się pozyskiwaniem wszelkich, powszechnie dostępnych informacji z ogólnie dostępnych, różnych źródeł jak np. państwowych i prywatnych środki masowego przekazu - celem wytworzenia sobie określonego obrazu sytuacji. Cenione są przeciwstawne informacje z odmiennych źródeł dające możliwość krytycznego podejścia do zgłębianej treści i opierając się na zasadach logicznego wnioskowania wykluczenia błędnych założeń i wersji, pozostawiając te najbardziej zbliżone do prawdy. Do źródeł białego wywiadu będzie również się zaliczał szeroko rozumiany wywiad środowiskowy czyli pozyskiwanie informacji o danej osobie lub instytucji na skutek zbierania opinii osób i podmiotów, które w jakikolwiek sposób zetknęły się z obiektem zainteresowania, lub posiadają o nim wyrobioną opinię na podstawie opinii innych osób. Wywiad środowiskowy może często prowadzić do mylnych wniosków, stąd konieczność weryfikacji uzyskanych tą drogą informacji innymi metodami – niemniej zdarza się, iż informacje pozyskane w ten sposób mogą się okazać niezwykle wartościowe. Ciekawostką jest, iż zdecydowana większość informacji pozyskiwanych przez wywiady różnych państw jest zdobywana w drodze białego wywiadu, natomiast jedynie niewielka ich część pochodzi ze źródeł powszechnie niedostępnych.<sup>19</sup>

Czarny wywiad gospodarczy – na gruncie prawa gospodarczego jest określane jako szpiegostwo gospodarcze i polega na nielegalnym pozyskiwaniu informacji. Można wyróżnić następujące metody przeprowadzenia czarnego wywiadu: wprowadzanie tzw. „kretów” czyli swoich pracowników do konkurencyjnej firmy pod pozorem zatrudnienia,<sup>20</sup> korupcja,<sup>21</sup> kradzież informacji,<sup>22</sup> szantaż,<sup>23</sup> oddziaływanie poprzez emocje i uczucia,<sup>24</sup> ekstremalnym przypadkiem – chociaż spotykanym zwłaszcza w krajach rozwijających jest porwanie i wymuszenie informacji w drodze zastraszenia lub tortur;<sup>25</sup> atak na systemy łączności – czyli podłączenie się do

<sup>19</sup> Według B. Jakubusa i M. Ryszkowskiego w ramach struktur wywiadowczych tajni współpracownicy dostarczają około 18% wszystkich informacji o dużej wartości (około 75-80% wartości na 100% wartości zdobytych informacji), natomiast reszta informacji jest pozyskiwana w drodze białego wywiadu i poddawana analitycznej obróbce (około 80% informacji o wartości 10-15% ogólnej wartości informacji). – Zob. B. Jakubus, M. Ryszkowski: *Ochrona informacji niejawnych*. Warszawa 2001

<sup>20</sup> Niezwykle skuteczne może się okazać wprowadzenie personelu sprzątającego biuro po wyjściu pracowników, gdyż osoby te z reguły budzą względne zaufanie i po opuszczeniu biura przez pracowników mają swobodny dostęp do większości pomieszczeń.

<sup>21</sup> Czynność tę musi poprzedzić dokładny wywiad o osobie, która ma zostać skorumpowana, tak aby wykluczyć potencjalne problemy, a nawet zdemaskowanie nieuczciwych zabiegów konkurencji.

<sup>22</sup> W znaczeniu tradycyjnym czyli kradzież określonej dokumentacji wyrażonej w postaci drukowanej, elektronicznego nośnika informacji lub innej możliwej do zabrania w drodze zwykłej kradzieży, napadu rabunkowego i włamania.

<sup>23</sup> Tę metodę stosuje się z reguły, gdy nie jest możliwe skorumpowanie danej osoby, lub osoba skorumpowana odmawia dalszej współpracy. Zasada jest taka, że rozwiązania siłowe zostawia się na sam koniec, gdy nie ma innej alternatywy pozyskania danej osoby i zarazem osoba ta jest niezbędna w realizacji danego zadania.

<sup>24</sup> Podstawienie atrakcyjnej partnerki, partnera osobie, której pozyskaniem jest zainteresowana konkurencja i poprzez nawiązanie więzi uczuciowej pozyskiwanie cennych informacji bez wzbudzania podejrzeń – tzw. casus Adama i Ewy.

<sup>25</sup> W przypadku, gdy działania takie zleciła konkurencyjna firma dbająca o swój nieskazitelny charakter w oczach partnerów biznesowych i opinii publicznej - albo tak stara się nakierować sprawę, aby media uznały to za samodzielne działania grup przestępczych, albo doprowadza do zaginięcia obiektu zainteresowania. Pomimo przerażającego charakteru opisanej metody – tragicznym i znanym przykładem możliwości jej zastosowania jest głośna od wielu lat sprawa porwania i zamordowania Krzysztofa Olewnika. Niemniej metoda musi się odnosić do informacji, których na bieżąco może udzielić porwana osoba, natomiast w przypadku większości z nich np. dokumentacji badawczej, strategii rozwoju danego działu firmy, stanu rozmów prowadzonych przez inne osoby – może okazać się chybiona.

ośrodków łączności danej firmy i prowadzenie nasłuchu prowadzonych rozmów telefonicznych celem zbierania informacji o wewnętrznych stosunkach w danej firmie; pewną odmianą będzie atak na elektroniczne komunikatory łączności jak GG czy Skype, co wchodzi już w pojęciowy zakres cyberprzestępczości.

Metody obrony przed zagrożeniami:

Obrona przed cyberprzestępczością:

- Utrzymywanie wewnętrznych sieci w ramach danego podmiotu gospodarczego, niemającej żadnej styczności z sieciami zewnętrznymi jak Internet. W przypadku połączenia jednego ze stanowisk z jakąkolwiek siecią zewnętrzną nieprzechowywanie na tym stanowisku żadnych, danych wrażliwych oraz odłączenie go na czas połączenia z siecią zewnętrzną, od sieci wewnętrznej. Ponowne włączenie do sieci wewnętrznej musiałyby nastąpić dopiero po dokładnym przeskanowaniu stanu danej jednostki. Miałyby to na celu wyeliminowanie sytuacji, w wyniku której jednostka podczas połączenia z siecią zewnętrzną została zainfekowana w taki sposób, że po odłączeniu od sieci zewnętrznej i włączeniu do wewnętrznej może ponownie nawiązać w określonym czasie połączenie z siecią zewnętrzną niezależnie od woli i wiedzy obsługi sieci wewnętrznej. Ewentualnie będąc włączona do sieci wewnętrznej gromadzi wszelkie informacje jakie są przez nią przesyłane na odrębnych obszarach pamięci, nie wykazywanych podczas rutynowych kontroli czy przeglądów i w momencie ponownego włączenia do sieci zewnętrznej – pomimo odłączenia od sieci wewnętrznej i pozornego oczyszczenia dysków – natychmiast transmituje dane z rezerwowych obszarów pamięci do określonej jednostki w sieci zewnętrznej. Jednak najpewniejszą metodą jest utrzymywanie sieci wewnętrznych, których jednostki nigdy nie będą łączone z sieciami zewnętrznymi, a do kontaktów z sieciami zewnętrznymi są wyselekcjonowane odrębne jednostki w żaden sposób nie stykające się z danymi wrażliwymi danego podmiotu gospodarczego.
- Utrzymywanie zespołu monitorującego sieci wewnętrzne, również pod kątem włamań mechanicznych, ale także jednostki mające łączność z sieciami zewnętrznymi pod kątem ich ochrony przed cyberatakami oraz szybkim i systematycznym wykrywaniem częstokrotności włamań. Wykrywanie ma istotne znaczenie praktyczne, gdyż częstokroć hakerzy dokonują kilkunastu, a czasem kilkudziesięciu nieudanych prób włamania zanim uda im się złamać zabezpieczenia. Dysponując sprawnym zespołem wykrywającym same przypadki prób naruszeń zabezpieczeń przez ingerencję zewnętrzną dysponuje się automatycznie większą ilością czasu na ustalenie konkretnego miejsca, jak i źródła ataku i ulepszeniem istniejących zabezpieczeń, zanim cyberprzestępcom uda się przeniknąć do zasobów danego podmiotu gospodarczego.

Obrona przed działalnością wywiadowczą (inaczej kontrwywiad):

- Kontrwywiad w zakresie białego wywiadu konkurencji – polega głównie na rzetelnej polityce informacyjnej firmy, natychmiastowym dementowaniu nieprawdziwych lub negatywnych informacji, kontroli przepływu informacji wewnątrz firmy i czuwaniem nad utrzymywaniem się pozytywnej opinii o miejscu pracy, także wśród samych pracowników.

- Kontrwywiad w zakresie czarnego wywiadu konkurencji – wymaga stworzenia instytucji wewnątrz firmy odpowiedzialnej za stworzenie systemu właściwego przepływu informacji zarówno jawnych, jak i wrażliwych dla firmy poprzez dwa odrębne systemy przekazu – Kancelaria Jawna i Kancelaria Tajna. Kontroli nad procesem rekrutacyjnym do firmy – poczynając od najniższych stanowisk, po najwyższe. Zapewnieniem właściwych form ochrony informacjom wrażliwym poprzez wyposażenie firmy w systemy alarmowe, monitoring, sejfy etc. pozwalająca na właściwe zabezpieczenie danych oraz kontrolę 24 godziny na dobę nad tym co się dzieje w firmie. Zatrudnienie profesjonalnej ochrony budynku. Odrębną działalnością kontrwywiadu w ramach firmy, ale niezwykle istotną z punktu widzenia jej interesów jest cicha i bieżąca obserwacja zatrudnionych w niej osób po względem: ich stanu majątkowego, relacji z innymi pracownikami, stopniem interesowania się sprawami firmy, podatnością na wpływ czynników zewnętrznych (wpływ innych ludzi, rewolucyjne idee, perspektywy rozwoju kariery zawodowej), stopień przywiązania do własnej firmy i cechy warunkujące to przywiązanie (np. solidarność, lojalność, finanse, kariera itd.). Reasumując kontrwywiad musi wiedzieć o wszystkim co dzieje się wewnątrz firmy, włącznie z nagłą zmianą zachowań pracowników (powinno wzbudzić podejrzenia, że cichy dotychczas pracownik działu kadr zaczyna dopytywać o szczegóły związane z zatrudnieniem poszczególnych osób, wczytuje się wnikliwiej niż dotychczas w dokumenty lub wnosi materiały tłumacząc to koniecznością pracy nad nimi w domu – zakładając, że wcześniej tego nie robił – niemniej może to oznaczać, że organizacja jego wewnętrznego czasu pracy z przyczyn zewnętrznych uległa zachwianiu – koniecznie jednak należy poddać takiego pracownika wnikliwszej niż dotychczas obserwacji).

Najlepszym podsumowaniem dla części tej pracy dotyczącej metod wywiadowczych i kontrwywiadowczych w gospodarce – oraz nawiązaniem do przedstawionych wyżej wyników Raportu McAfee są słowa cytowanego już wcześniej funkcjonariusza odpowiadającego za ochronę łączności w ramach jednej z instytucji bezpieczeństwa publicznego – „Najczęstszym powodem wycieku danych z systemów łączności i przechowywania informacji jest to, że zawinił czynnik ludzki”. Niejako potwierdzeniem jest notatka prasowa, która ukazała się na portalu internetowym wp.pl informująca o wynikach badania „E-crime Survey 2009”, które zostały przedstawione podczas Kongresu E-Crime w Londynie. Badanie objęło 307 firm z sektora prywatnego, organizacji rządowych oraz agencji ds. walki z przestępczością i wykazało, iż około 66% respondentów biorących udział w badaniu KPMG/ stwierdziło, że zwolnieni z pracy i pozbawieni perspektyw specjaliści branży IT mogą zdecydować się na nielegalną działalność, która szybko przyniesie im spore zyski. Analitycy stwierdzili, że pracownicy zatrudnieni w sektorze IT mają stosunkowo łatwy dostęp do struktur systemów firm i doskonale znajdują ich słabości. Zdaniem analityków firmy powinny zapewnić sobie jasną procedurę postępowania, w sytuacji gdy taka osoba przestanie pracować dla firmy.<sup>26</sup> W moim przekonaniu pewne, gotowe rozwiązania mogłyby przynieść mechanizmy funkcjonowania kan-

<sup>26</sup> Zwolnieni pracownicy IT – potencjalni przestępcy, wp.pl, <http://tech.wp.pl/kat,39516,title,Zwolnieni-pracownicy-IT-potencjalni-przestepcy,wid,10979780,wiadomosc.html?ticaid=17bfd> (pobrano 29.03.2009)

celarii tajnych – przy adaptacji do uwarunkowań konkretnych podmiotów gospodarczych. Pewnym pocieszeniem natomiast, może być fakt, iż często młodzi i inteligentni ludzie, którzy w odpowiednio młodym wieku potrafili zgłębić tajemnice współczesnej informatyki są zatrudniani jako specjaliści ds. cyberprzestępczości i cyberterroryzmu. Doskonałym przykładem jest historia Owena Thor Walkera, nastoletniego hakera z Nowej Zelandii, który został konsultantem do spraw cyberprzestępczości w jednej z największych firm telekomunikacyjnych w kraju. Pozostaje mieć nadzieję, że w przyszłości to struktury państwowe będą wyprzedzać potencjalne działania przestępcze opracowując na wyrost odpowiednie strategie działania – a nie na odwrót.