Aleksander Chmiel

Przestępstwa związane z wykorzystaniem komputera : charakterystyka zagadnienia

Palestra 35/10(406), 12-19

1991

Aleksander Chmiel

Przestępstwa związane z wykorzystaniem komputera

- charakterystyka zagadnienia

Ataki na system komputerowy są coraz częstsze; zdarzają się też w Polsce.[1] Zdaniem G. Kaisera, stwarzają one zagrożenia zarówno dla gospodarki prywatnej, jak i dla państwowej. Jednym z takich zagrożeń jest nielegalne wprowadzanie zmian w zapisie danych przez pracowników. Stwarza to nowe problemy dla prawa karnego, gdyż należy się spodziewać wzrostu liczby przypadków manipulacji komputerowych.[2]

Istnienie tego zagrożenia jest realne, gdyż np. w 1980 r. RFN miała już około 30 tys. systemów komputerowych, a w tym samym czasie w USA znajdowało się w użyciu 5-6 mln sztuk komputerów.[3] A przecież przewrót w elektronice dopiero wtedy się rozpoczął.

W literaturze wyróżnia się trzy grupy czynów szkodliwych dla prawidłowego obiegu informacji. Są to następujące czyny (przypadki):

1) manipulowanie komputerem,

2) niszczenie informacji lub programu (sabotaż komputerowy),

3) bezprawne uzyskiwanie informacji (szpiegostwo komputerowe).

Oczywiste jest, że komputer (lub jego urządzenie peryferyjne) może, tak jak każda inna rzecz, ulec zniszczeniu, zostać skradziony, uszkodzony, itp. Całkowitemu lub częściowemu zniszczeniu mogą ulec informacje fabryczne wprowadzone do sprzętu komputerowego (*hardware*). Jednakże w dalszej części rozważań chciałbym się skupić nad problematyką związaną z tzw. oprogramowaniem (*software*).[5]

Ad 1/ Manipulowanie komputerem

Aby komputer właściwie pracował muszą być spełnione następujące warunki:

a) musi być zastosowany właściwy program,

b) właściwe dane (informacje) muszą zostać wprowadzone do komputera,

c) musi być właściwie obsługiwane urządzenie „wejścia - wyjścia" (np. konsola, monitor, terminal),

d) właściwe dane (informacje) muszą być wyprowadzone z komputera.[6]

A. Manipulowanie programem. Najczęściej polega to na wprowadzeniu do programu instrukcji aby komputer „wpłacał" na jakieś konto niewielkie kwoty np. kilkudolarowe „końcówki". W USA miał miejsce przypadek, gdy programista tak zmienił program, że na jego konto wpływały stale niewielkie kwoty, a bilans banku nie wykazywał ujemnego salda. Sprawa została ujawniona, gdy bank musiał dokonać łącznego przeliczenia wszystkich kont

w sposób przyjęty przez tradycyjną księgowość.[7]

B. Manipulowanie „na wejściu" (*Input*). Jest to chyba najprostsza i najstarsza z możliwości popełniania przestępstw przy użyciu komputera, gdyż sięga epoki kart perforowanych. W USA sposób ten wykorzystywany jest w oszustwach podatkowych. Nie chodzi tu o podawanie fałszywych danych, lecz o takie sfałszowanie informacji na karcie perforowanej czy taśmie magnetycznej, że operacje rachunkowe dokonane przez komputer uwzględniają np. nienależne sprawcy czy osobie trzeciej zniżki lub zwolnienia podatkowe.

Czasami sprawca wprowadza do programu komputerowego „podprogram" (tzw. wstawkę), który aktywizuje się dopiero po kilku miesiącach, gdy np. programista już nie pracuje w tym banku.

C. Manipulowanie konsolą lub innym urządzeniem służącym do wydawnia poleceń komputerowi. Występuje najczęściej wtedy, gdy komputer pracuje w systemie wielodostępnym lub (i) w sieci komputerowej (współpracuje z innymi komputerami). W jednym z niemieckich banków, który współpracując z bankami innych krajów przeprowadzał operacje dewizowe, pracownik przywłaszczył kwotę około 25 mln DM. Polegało to na tym, że pracownik ten, wykorzystując wahania kursów walut, obracał kapitałem banku zysk zachowując dla siebie. Nigdy nie udało się ustalić, który z 80 pracowników banku wykorzystywał w ten sposób swój komputer.[8]

D. Manipulowanie „na wyjściu" (*Output*). Często polega to na wystawianiu tzw. podwójnych rachunków - rachunek na inną kwotę otrzymywał klient, a do pamięci komputera zostaje wprowadzona inna kwota; różnicę zagarnia np. sprzedawca.

Przedstawione tu przypadki (czyny) bardzo rzadko występują w „czystej" postaci, gdyż poszczególne czynności najczęściej przeplatają się.

Ad 2/ Niszczenie informacji (sabotaż komputerowy). Przestępstwo to polega na niszczeniu danych z zamiarem szkodzenia stosunkom majątkowym pokrzywdzonego. Oto kilka przykładów:

- w USA opiekunka „magnetycznej biblioteki" z zemsty zniszczyła taśmy magnetyczne; strata wyniosła 10 mln dolarów,
- w 1970 r. grupa przeciwników wojny wietnamskiej i terrorystów spowodowała eksplozję we współpracującym z armią centrum komputerowym Uniwersytetu Wisconsin. Strata wyniosła 1 mln dolarów (zniszczono taśmy magnetyczne zawierające dane zbierane od 20 lat).[9]

Obecnie nie ma powodu i potrzeby niszczenia samego sprzętu komputerowego (*Hardware*), gdyż znacznie bardziej dotkliwe jest dla właściciela czy użytkownika zniszczenie danych zawartych w pamięci komputera, np. na dyskach, taśmach magnetycznych lub na dyskietkach.

Najwięcej szkód przysparza wprowadzenie do programu specjalnego podprogramu ("wirusa"), który zniekształca dane, zmienia je często w sposób trudno dostrzegalny, oddziaływując przy tym na cały system komputerowy, w którym pracuje „zarażony" komputer.

Istnieją różne możliwości niszczenia danych. Np. programista opracowujący na zlecenie program koduje w nim inny podprogram, który ma zniszczyć zawarte w komputerze dane, jak też inne wykorzystywane w tym komputerze programy. Program może być też prawidłowy, lecz osoba obsługująca komputer może zmienić go na samoniszczący. Największe niebezpieczeństwo zagraża od osób (tzw. hackerów), które po przełamaniu zabezpieczenia uniemożliwiającego wprowadzenie danych do systemu komputerowego przez osoby niepowołane

wprowadzają swój podprogram ("wirus"). Często są to młodzi ludzie, których celem nie jest niszczenie danych, ciekawi ich tylko, jak zachowa się „wirus". Niektórzy z nich to „maniacy komputerowi", osobnicy chcący dowieść sobie i światu siły swego intelektu. Najwięcej kontrowersji wzbudza fabryczne wprowadzanie przez producentów podprogramu, który uaktywnia się po nielegalnym skopiowaniu programu.[10]

Ad 3/ Bezprawne uzyskiwanie informacji (szpiegostwo komputerowe). Polega ono na bezprawnym uzyskaniu i zużytkowaniu danych. U. Sieber uważa, że powinno to również spowodować straty majątkowe u pokrzywdzonego.[11]

W wielu przypadkach chodzi tu o takie zakodowane dane, jak: adresy klientów, bilans firmy, wysokość płaconych podatków, receptura, technologia, lista płac. Celem sprawcy może być też uzyskanie samego programu komputerowego, czy to produkowanego przez daną firmę, czy też tylko przez nią używanego, np. do prowadzenia księgowości. Odrębne zagadnienie to bezprawne uzyskiwanie danych gospodarczych czy militarnych przez włączenie się do sieci komputerowej agentów obcego państwa.

Oprócz tych typowych czynów można wyróżnić także i inne, które wprawdzie cechuje znacznie mniejszy ładunek społecznego niebezpieczeństwa,lecz ich nagminność wymaga zastanowienia się nad problemem ich występowania. A oto przykładowo kilka z nich.

Kradzież czasu pracy. Powszechnie wiadomo, że osoby obsługujące sprzęt komputerowy często dokonują na nim obliczeń na własny użytek lub też na zlecenie innych osób. Korzystają przy tym ze sprzętu stanowiącego własność firmy, w której są zatrudnieni, zużywają energię elektryczną, czasem odbierają tej firmie klientów. Obliczeń dokonują często w czasie godzin pracy.

Kopiowanie programów. Może mieć ono charakter nieodpłatny - na potrzeby własne lub znajomych (głównie gry komputerowe). Niekiedy jednak celem jest osiągnięcie zysków z wielokrotnego kopiowania szczególnie atrakcyjnego programu. Tak skopiowany program sprzedawany jest jako oryginalny (ale za to znacznie taniej) i zaopatrzony w znak firmowy producenta. Wykorzystywane do kopiowania urządzenia są niejednokrotnie własnością pracodawców „producentów". Pojawia się więc znowu problem kradzieży czasu pracy, energii elektrycznej itp.

Publiczne i odpłatne wykorzystywanie programów komputerowych mimo że producent zastrzegł sobie zakaz takich praktyk. Dotyczy to głównie prowadzenia kursów czy korepetycji, np. z fizyki lub chemii.

1. *Regulacje prawne*

W wielu krajach (np. Austrii, Francji, Wielkiej Brytanii, Niemczech, Japonii, USA) nastąpiła penalizacja czynów będących atakami na systemy komputerowe.

W USA w 1977 r. złożono w senacie projekt federalnego aktu prawnego, który dotyczył tzw. przestępstw komputerowych. Kongres USA nie uchwalił go jednak, gdyż przewidywał zbyt wysokie kary - do 15 lat pozbawienia wolności. Po pewnych zmianach i obniżeniu górnego zagrożenia do lat 5 uchwalono w 1979 r. *Federal Computer System Protection Act*,[12] w którym określono nowe czyny przestępne - komputerowe oszustwo i nadużycie (*Computer Fraud and Abuse*). Przepisy tam zamieszczone nie mogły znaleźć szerszego zastosowania, chociażby z uwagi na szereg wyłączeń. Wyłączenia te wynikają np. z określenia przez ustawodawcę definicji komputera: „urządzenie, które przeprowadza logiczne, arytmetyczne i służące do przechowywania danych operacje elektroniczne /.../, ale nie jest elektroniczną drukarką

lub maszyną do pisania /.../, nie jest też elektronicznym kalkulatorem kieszonkowym z ręczną obsługą".[13] Ustawodawca wymaga też, aby komputer był w posiadaniu albo był zakontraktowany (wykonywał obliczenia) przez rząd USA lub instytucję finansową wymienioną w ustawie. Zakazane postępowanie musi wpływać bezpośrednio na działanie tego komputera.[14] Tak skonstruowana ustawa mogła być stosowana tylko w przypadku popełnienia najcięższych przestępstw i z racji wyłączeń nie spełniała swego zadania. W 1984 r. uchwalono ustawę, która penalizuje także oszustwa i nadużycia dokonane za pomocą komputera w stosunku do innych instytucji oraz osób fizycznych. Penalizacja objęła także uzyskiwanie zakodowanych informacji przez osoby do tego nie uprawnione (głównie chodziło tu o uzyskiwanie informacji przez firmy konkurencyjne).

Inaczej problem ten został rozwiązany w ustawodawstwie niemieckim. W dniu 15 maja 1986 r. uchwalono *Zweites Gesetz zur Bekämpfung der Wirtschaftkriminalität,* która weszła w życie 1 sierpnia 1986 r. Wśród przepisów dotyczących przestępczości gospodarczej zawarte są też uregulowania dotyczące przestępstw komputerowych.[15] Kluczowy jest §202 a (2) StGB, w którym określono pojęcie „dane": są to „tylko takie dane elektroniczne, magnetyczne lub inaczej niż bezpośrednio postrzegane dane, które zostały zgromadzone albo miały być przekazane". W StGB określono jedenaście nowych typów czynów zabronionych, które mają związek z wykorzystaniem urządzeń komputerowych. Można je jednak pogrupować, stosując podział przestępstw komputerowych przedstawiony na początku tych rozważań.[16] Dla ustawodawcy niemieckiego nie jest najważniejsze to, w czyim posiadaniu znajduje się komputer i na czyją rzecz pracuje. Nie jest też określone, co należy przez pojęcie „komputer" rozumieć (tj. rodzaj urządzenia elektronicznego). Istotne, czy zniszczone, przekazane czy w inny sposób wykorzystane informacje miały charakter „danych", o których mowa w §202 a StGB.

Zarówno w USA, jak i RFN penalizuje się tylko czyny popełnione z winy umyślnej. Usiłowanie jest karalne. Należy się jednak spodziewać, że wraz ze wzrostem wykorzystania urządzeń komputerowych we wszystkich dziedzinach życia (np. w wojskowości, energetyce jądrowej) penalizowane będą także i czyny będące wynikiem niezachowania obowiązku wymaganej ostrożności, tj. popełnione z winy nieumyślnej.

2. *„Przestępstwa komputerowe" w świetle polskiego prawa karnego*

Czy obecnie obowiązujące polskie prawo karne może być skutecznym narzędziem w zwalczaniu „przestępstw komputerowych"? Należy na to pytanie odpowiedzieć przecząco. A przecież różnego rodzaju urządzenia elektroniczne wykorzystywane są także i w naszym kraju, ich liczba ciągle wzrasta i nie można traktować możliwości wykorzystywania ich dla celów przestępnych jako abstrakcyjnej. Problem ten dostrzegła Komisja d/s Reformy Prawa Karnego, wprowadzając w projekcie z marca 1990 r. pojęcie przestępstwa oszustwa komputerowego, a w projekcie z sierpnia 1990 r. penalizując także przypadki uzyskiwania zakodowanych informacji przez osoby do tego nie uprawnione.

Oczywiste jest, że problemu popełnienia „przestępstw komputerowych" nie należy demonizować, tym bardziej, że mogą ukształtować się odmienne typy zachowań społecznie niebezpiecznych, specyficzne dla Polski, a nie znane w innych krajach.

Problematyka „przestępstw komputerowych" jest, jak to wykazano wyżej, skomplikowana, dlatego trudno pokusić się o wyjaśnienie wszystkich istotnych kwestii. Z konieczności ograniczam się do przedstawienia najistotniejszych problemów.

Oszustwo komputerowe. Celem sprawcy jest w tym przypadku osiągnięcie korzyści majątkowej poprzez zmianę danych, niewłaściwe ich użycie, posługiwanie się niepełnymi danymi lub niewłaściwie skonstruowanym programem. Komputer może więc być wykorzystywany przez sprawcę jako narzędzie służące do wprowadzenia innej osoby w błąd lub do wykorzystania błędu, gdy podjęcie decyzji rozporządzającej mieniem należy do człowieka. W tej sytuacji art. 199 k.k. czy art. 205 k.k. mogą znaleźć zastosowanie. Problem komplikuje się jednak wtedy, gdy decyzja, wskutek której dochodzi do rozporządzenia mieniem należy nie do człowieka, lecz podejmowana jest na podstawie danych wprowadzonych przez urządzenie elektroniczne. W tym przypadku wymienione przepisy nie mogą być stosowane. W art. 205 k.k. ustawodawca mówi o doprowadzeniu „innej osoby" do niekorzystnego rozporządzenia mieniem, określając w ten sposób definicję oszustwa. Definicja ta wyjaśnia także pojęcie oszustwa użyte przez ustawodawcę w §8 art. 120 k.k.[17]

Tak zwane oszustwa komputerowe mimo znacznego ładunku społecznego niebezpieczeństwa nie stanowią w obowiązującym obecnie w Polsce systemie prawnym przestępstwa; brak jest bowiem zakazu ustawy (znamienia bezprawności). Gdyby więc ktoś popełnił taki czyn, nie mógłby być ścigany karnie (chyba że naruszył także inne normy), a sąd powinien wydać wyrok uniewinniający. Pokrzywdzony mógłby dochodzić zwrotu swego mienia tylko na drodze procesu cywilnego. Ten stan prawny jest wielce niekorzystny i wymaga modyfikacji, mimo że zagrożenie w postaci czynów jest obecnie w naszym kraju minimalne. Nie można go jednak lekceważyć.

Należy też odpowiedzieć na pytanie, czy „oszustwo komputerowe mieści się w pojęciu "zagarnięcia", a ściślej mówiąc w określeniu „inne wyłudzenie" (art. 120 §8 k.k.). Istnieją z pewnością elementy odróżniające „inne wyłudzenie" od „oszustwa", jednakże stanowisko doktryny nie jest tu jednoznaczne. J. Bednarzak uważa, że różnica sprowadza się do faktu, czy korzyść jest skutkiem doprowadzenia kogokolwiek do wydania decyzji rozporządzającej mieniem. Decyzja taka w przypadku „innego wyłudzenia" nie jest niekorzystna w chwili jej wydania, nie jest też wywołana przez podstępne działanie sprawcy.[18]

Obecnie nasilają się tendencje do zrównania ochrony prawno-karnej wszystkich form własności (ustawa z 23 lutego 1990 r. o zmianie kodeksu karnego i niektórych innych ustaw - Dz.U. Nr 14, poz. 84). Należy więc przypuszczać, że ustawodawca powróci do tradycyjnych określeń sposobów działania sprawców przestępstw przeciwko mieniu (kradzież, przywłaszczenie, oszustwo, sprzeniewierzenie itp.), a wzbudzające kontrowersje „inne wyłudzenie" zostanie wyeliminowane. Z tej to przyczyny problem ten jedynie zasygnalizowano.

Opierając się na tradycyjnym ujęciu przestępstwa oszustwa (art. 205 k.k.), w którym nie mieszczą się stany faktyczne stanowiące „przestępstwo oszustwa komputerowego", konieczne staje się uzupełnienie tego przepisu w taki sposób, aby swym zakresem obejmował także i te przypadki. Proponuję dodanie po §1 art. 205 k.k. §2 (dotychczasowy §2 art. 205 k.k. otrzyma numerację §3) w następującym brzmieniu: „tej samej karze podlega ten, kto w celu osiągnięcia korzyści majątkowej wskutek pokrzywdzenia innej osoby manipuluje urządzeniem komputerowym zmieniając dane, niewłaściwie ich używając, posługując się niepełnymi danymi lub błędnie skonstruowanym programem".[19]

Niszczenie informacji lub programu (sabotaż komputerowy) wykazuje podobieństwo do innych stanów faktycznych takich, jak: niszczenie zapisu dźwiękowego na taśmie magnetycznej, obrazu na taśmie

video czy taśmie filmowej. Charakterystyczne dla „sabotażu informatycznego" jest to, że często dla jego dokonania wystarczająca jest tylko zmiana czy nawet przestawienie kolejności danych oraz fakt, że wprowadzenie dodatkowych danych może zniszczyć nie tylko informacje zawarte w danej dyskietce czy taśmie magnetycznej, lecz może spowodować blokadę całej sieci informatycznej, działając niszcząco na wszelkie zgromadzone dane.[20] Sytuacja taka może wywołać poważne zakłócenia w pracy instytucji, w której dane są wykorzystywane lub gromadzone, a nawet oddziaływać na całą gałąź gospodarki. Dlatego nie bez znaczenia będzie tu motywacja sprawcy. Celem jego postępowania może być np. wywołanie poważnych zakłóceń w funkcjonowaniu gospodarki (art. 127 k.k.), zniszczenie mienia (art. 212 k.k.), spowodowanie zakłóceń w działalności gospodarczej, komunikacji lub łączności (art. 220 k.k.).

Nasuwa się pytanie, co jest przedmiotem ochrony w tych przykładowo wymienionych typach czynów zabronionych? Czy dobrem chronionym jest tu mienie lub prawidłowe działanie gospodarki? Jeśli tak, to czy jest to dobro główne? Opowiadając się za takim ujęciem traktujemy prawidłowy obieg informacji jako dobro uboczne.[21] Wydaje się jednak, że specyfika czynów skierowanych przeciwko prawidłowemu obiegowi informacji z racji choćby niewymierności (lub trudności w ustaleniu) szkód czyni dobra te co najmniej równorzędnymi. Przyjmując takie rozwiązanie należałoby konsekwentnie wprowadzić do kodeksu karnego odrębny rozdział, w którym czyny te byłyby stypizowane. Za takim uregulowaniem przemawia także i to, że wielu stanów faktycznych nie obejmują swym zakresem obowiązujące normy prawne.

Kolejny problem związany z niszczeniem danych (informacji) wiąże się z określeniem ich wartości. Według jakich kryteriów należy ją oceniać? Wyobraźmy sobie sytuację, gdy ktoś niszczy (kasuje) bardzo istotne dane zapisane w pamięci komputera. Użytkownik komputera ma jednak kopię tych danych zapisaną na dyskietce. Ponowne wprowadzenie ich do pamięci zajmie mu kilka sekund. Pewne wątpliwości nasuwają się w przypadku, gdy dane te nie są zapisane na dyskietce, lecz trzeba je odtwarzać z dokumentacji, programując komputer ponownie. Czy ich wartość trzeba oceniać w zależności od czasu, jaki poświęcono na ponowne ich wprowadzanie?

A jeśli nawet ponowna rejestracja danych nie łączyła się ze znacznymi kosztami, to czy wartość zniszczonych informacji nie należy oceniać uwzględniając także realnie oczekiwane korzyści (*locrum cessans*)?[22]

Wiele z tych pytań może znaleźć odpowiedź dopiero wtedy, gdy ukształtuje się praktyka orzekania w tego typu sprawach. Jednakże konieczne wydaje się uprzedzenie przez ustawodawcę tej sytuacji poprzez stypizowanie przedstawionych wyżej stanów faktycznych. W rozważaniach zasygnalizowano pewne problemy, które mogą wyniknąć w trakcie praw ustawodawczych.

B e z p r a w n e u z y s k i w a n i e i n f o r m a c j i (s z p i e g o s t w o k o m p u t e r o w e). Uwagi odnoszące się do rodzaju dobra prawnego chronionego przez przepisy karne odnoszą się także i do tych przypadków. Ze względu na toczące się prace legislacyjne nie będę szczegółowo omawiał tego problemu.

Za konieczne uważam takie przekształcenie art. 172 k.k. (naruszenie tajemnicy korespondencji), aby obejmował on swym zakresem także przynajmniej niektóre stany faktyczne związane z elektronicznym przekazywaniem danych.

Zwrot „do podawania wiadomości" proponuję zastąpić określeniem „do przekazywania informacji". Po słowach „przy użyciu środków telekomunikacji" proponuję dodanie zwrotu „lub innych urządzeń służących do przekazywania danych elektronicznych". Wszędzie tam, gdzie w art. 172 k.k. występuje pojęcie

„wiadomości" powinno być ono zastąpione pojęciem „informacja".[23]

Proponowane zmiany mają nie tylko charakter kosmetyczny i nie chodzi tu też tylko o uczulenie wymiaru sprawiedliwości na możliwość zastosowania art. 172 k.k. w sytuacji, gdy sprawca podłączył się do sieci komputerowej. Pojęcie „informacja" jest, moim zdaniem, pojęciem szerszym od pojęcia „wiadomość", gdyż obejmuje także i przekazywanie obrazu, co z racji na coraz częstsze stosowanie telefaksu nie będzie bez znaczenia. Z kolei wprowadzenie „innych urządzeń służących do przekazywania danych elektronicznych" obejmuje także i taki stan faktyczny, gdy ktoś włącza się do sieci komputerowej, jaką posługuje się dana instytucja. W żadnym przypadku takie wewnętrzne połączenia nie są „środkiem telekomunikacji", którego to określenia używa ustawodawca w art. 172 k.k.

Jak wykazano wyżej, istnieje potrzeba prawnego uregulowania problemów powstałych wskutek rozwoju elektroniki. Ponieważ zagadnienie to jest bardzo obszerne i skomplikowane, przedstawiam tylko niektóre z jego aspektów. Wiele z nich wymaga szerszego omówienia, co jednak przekracza ramy tego opracowania, w niczym nie umniejszając przy tym ich wagi.

Przypisy

[1] Ile takich przypadków miało miejsce w Polsce nie wiadomo, jednakże zagrożenie takie istnieje. Jeden z takich przypadków miał miejsce we wrześniu 1989 r. i wzbudził pewne kontrowersje; patrz J. D z i a d u l: Znikająca pamięć, „Polityka" z 9.XII.1989 r. nr 49.

[2] G. K a i s e r: Przestępczość gospodarcza: zjawisko, zapobieganie w republice Federalnej Niemiec, NP z 1989 r. nr 2-3, s. 186.

[3] Trudno podać tu dane dotyczące Polski, gdyż, jak wiadomo, urządzenia elektroniczne były sprowadzane głównie przez osoby prywatne.

[4] U. S i e b e r: Computerkriminalität und Strafrecht, Köln-Berlin-Bonn-München 1977, s. 39-40.

[5] Jest to zbiór programów i podprogramów umożliwiających eksploatację komputera. Por. H. J e z i e r s k a: Słownik informatyki, Warszawa 1989 r.

[6] U. S i e b e r: op.cit., s. 42.

[7] Tamże, s. 54-57.

[8] Wysoko kwalifikowani zawodowo sprawcy wymagają wyspecjalizowanych organów ścigających tego typu przestępstwa. Np. w USA działa „policja informatyczna" - *Computer Fraud Departament*

[9] U. S i e b e r: op.cit., s. 88.

[10] J. B u l i k: Gdy komputer ma grypę, „Polityka" z 23-30.XII. 1989 r. nr 51-52.

[11] U. S i e b e r: op.cit., s. 98. Por. też: T. L e c n e r: Computerkriminalität und Vrmogensdelikter, Heidelberg-Karlsruhe 1981, s. 17.

[12] Przepisy te zostały włączone do tzw. wzorcowego kodeksu karnego USA (*Criminal Code*) jako §1028. Przewidziano następujące kary: grzywna nie większa niż dwukrotna uzyskana korzyść lub grzywna do 50 tys. dolarów, w zależności od tego, która z tych kar będzie większa, lub kara pozbawienia wolności do lat 5, albo obie kary łącznie.

[13] *Computer Fraud and Abouse* §1028(c) „Definitions: computer".

[14] §1028 (a).

[15] Ustawa ta zmieniała szereg przepisów niemieckiego kodeksu karnego (StGB), wprowadziła też nowe typy czynów zabronionych.

[16] Por. też. R. M ü l l e r, H. B. W a b n i t z: Wirtschaftskriminalität, München 1986, s. 209-212.

[17] Por. np. J. B a f i a, K. M i o d u s k i, M. S i e w i e r s k i: Kodeks karny, Komentarz, Warszawa 1977, s. 507.

[18] J. B e d n a r z a k: Przestępstwo oszustwa w polskim prawie karnym, Warszawa 1971, s. 150-152.

[19] Ponieważ nie znam ostatecznej wersji projektu (nie została opublikowana), nie chcę tu ustosunkowywać się do rozwiązań proponowanych w nieaktualnych już projektach.

[20] Straty stąd wynikające mogą być bardzo wysokie, gdyż sprawcy często skutecznie szantażują instytucje, grożąc im zniszczeniem danych.

[21] Co do rozróżnienia głównych i ubocznych dóbr chronionych patrz np. K. B u c h a ł a: Prawo karne materialne, Warszawa 1989, s. 196-200

[22] Problematyczne jest, czy należy brać pod uwagę wartość mienia czy wysokość szkody.

[23] Patrz przyp. 19.