Transport poczty elektronicznej

podstawowe zagadnienia, problemy, rozwiązania

Marcin Goliszewski <m.goliszewski@ii.pw.edu.pl>

Streszczenie

Niniejszy artykuł prezentuje przegląd zagadnień technicznych, a także zjawisk kulturowo-społecznych związanych z transportem poczty elektronicznej. Zostaje w skrócie zaprezentowana historia oraz ewolucja protokołów do tego celu przeznaczonych, a także sytuacja panująca współcześnie na rynku poczty elektronicznej – stosowane protokoły oraz związane z nimi występujące problemy. Na zakończenie zaprezentowana zostaje również propozycja systemowego, choć rewolucyjnego i odważnego, ich rozwiązania.

1. Historia poczty elektronicznej

Poczta elektroniczna jest jednym z ważniejszych narzędzi współczesnej komunikacji między użytkownikami komputerów. We współczesnym świecie istnienie i używanie poczty elektronicznej jest tak naturalne, że stała się ona częścią codziennego życia wielu ludzi. Jako coś bardzo powszedniego, niewiele osób zastanawia się nad jej historią, gdyż nie sądzą, że może ona być im do czegokolwiek przydatna. Moim zdaniem, poznanie sposobu, w jaki przebiegał rozwój poczty elektronicznej, a także protokołów jej wymiany, jest bardzo istotne z punktu widzenia oceny jej obecnego stanu, a także zrozumienia zjawisk na współczesnym rynku pocztowym występujących.

Historia poczty elektronicznej rozpoczyna się o wiele wcześniej niż termin ten został stworzony. Pierwszym krokiem do wymiany wiadomości między użytkownikami systemu komputerowego było powstanie systemu wielodostępnego, na którym wiele osób mogło pracować jednocześnie. Systemem, który odegrał istotną rolę w rozwoju komunikacji elektronicznej, był **C**ompatible **T**ime-**S**haring **S**ystem oddany do użytku w 1961 r. [1] w Massachusetts Institute of Technology. System ten został stworzony z myślą o zdalnym dostępie użytkowników z terminali podłączanych za pośrednictwem m.in. sieci telefonicznej. Jedną z głównych usług udostępnianych przez CTSS była możliwość zapisywania i odczytywania plików przechowywanych na dysku serwera. Użytkownicy szybko zaczęli możliwość tą wykorzystywać w sposób odmienny niż założyli sobie administratorzy serwera – oprócz współdzielenia plików projektów, nad którymi wspólnie pracowali, zaczęli w katalogach grup projektowych zostawiać sobie wiadomości. Były one prostymi plikami tekstowymi, w których wpisana była treść wiadomości. Prymitywne „adresowanie" zrealizowane zostało przez nadawanie plikom wiadomości znaczących nazw, np. `TO TOM`. Obserwując ten trend, administratorzy CTSS postanowili stworzyć narzędzie, które ułatwiałoby komunikację między użytkownikami, a także umożliwiłoby proste wysyłanie wiadomości od administratorów do szerszej grupy użytkowników. Na przełomie lat 1964/1965 powstał pomysł stworzenia narzędzia `MAIL`, które miało powyższe zadania realizować. Pozwalało ono dowolnemu użytkownikowi CTSS wysłać wiadomość do dowolnego innego użytkownika, pod warunkiem znania symbolu projektu oraz numeru użytkownika adresata.

Podobnych do istniejącego w MIT CTSS systemów lokalnej wymiany wiadomości między użytkownikami jednego systemu powstało wiele. Jednym z nich był system oparty o program `SENDMSG` działający w systemie TENEX stworzonym przez Digital Equipment Company. Początkowo jego możliwości były praktycznie identyczne, jak możliwości programu `MAIL` z CTSS. W połowie 1971 r. Ray Tomlinson z DEC postanowił rozszerzyć możliwości programu `SENDMSG` o opcję wymiany wiadomości między zdalnymi systemami, co opisuje w [2]. Opracował w tym celu protokół CPYNET – prosty protokół przesyłania plików między zdalnymi systemami, który zastosowany mógł zostać również do zapisywania wiadomości wysłanych przy pomocy programu `SENDMSG` do skrzynek pocztowych użytkowników na zdalnych komputerach z systemem TENEX. Przy okazji opracowywania tego systemu wymiany wiadomości, jego autor podjął jedną decyzję projektową, której skutki do dnia dzisiejszego widoczne są podczas codziennego korzystania z poczty elektronicznej: zadecydował, iż wiadomości od lokalnych użytkowników będą odróżniane od wiadomości od zdalnych użytkowników poprzez dodanie do nazwy nadawcy tych drugich znaku „`@`" i nazwy komputera, z którego wiadomość została wysłana. Ten format zapisu został następnie usankcjonowany jako obowiązujący w sieci ARPANET, a później również Internet, przez różne dokumenty standaryzujące (m.in. RFC 2822 [3]). Pierwsze wiadomości

przesłane między zdalnymi komputerami (fizycznie zlokalizowanymi tuż koło siebie, ale w sensie logicznym połączonymi jedynie poprzez sieć ARPANET) za pomocą tego protokołu zostały pod koniec roku 1971 – początkowo były to typowo testowe ciągi znaków (prawdopodobnie `QWERTYUIOP` lub podobne, ale dziś nie sposób już tego z całą pewnością stwierdzić). Pierwszą wiadomością niosącą sensowną treść było obwieszczenie powstania sieciowej poczty elektronicznej skierowane do użytkowników systemu TENEX, wraz z krótką instrukcją obsługi nowych funkcji programu `SENDMSG`. Za ciekawostkę można uznać fakt, iż prace nad tym systemem wymiany poczty nie odbywały się na zlecenie firmy DEC, a wręcz przeciwnie – początkowo Tomlinson pracował wręcz w tajemnicy przez swoimi zwierzchnikami. Jedynym uzasadnieniem, które podaje on na rozpoczęcie prac nad nową wersją `SENDMSG`, jest: *„mostly because it seemed like a neat idea”* („głównie dlatego, że wydawało się to niezłym pomysłem”).

Równocześnie z wydaniem wersji systemu TENEX zawierającej możliwość przesyłania poczty elektronicznej między zdalnymi systemami, rozwiązanie stworzone przez Raya Tomlinsona powielił Abhay Bhushan, wykładowca MIT, w stworzonym przez siebie **F**ile **T**ransfer **P**rotocol dla sieci ARPANET. Miało to bardzo istotne znaczenie dla rozwoju komunikacji sieciowej, gdyż protokół ten stał się pierwszym standaryzowanym (w RFC 354 [4]) protokołem umożliwiającym transport poczty elektronicznej. Jednakże wraz ze wzrostem liczby użytkowników tej usługi, Bhushan doszedł do wniosku, iż w momencie, kiedy transport poczty elektronicznej stał się zbyt istotnym elementem aktywności w sieci ARPANET, aby być jedynie „dodatkiem” do protokołu przesyłania plików, należało opracować jeden, wspólny dla całej sieci, standard jej transportu. W związku z tym stanął on na czele komitetu, którego celem było opracowanie wspólnego standardu dla wszystkich systemów podłączonych do sieci ARPANET. Niestety okazało się to o wiele trudniejsze, niż by się wydawało – w ciągu pierwszych czterech lat prac (tj. między 1973 r. a 1977 r.) powstały aż cztery propozycje standardów dotyczących formatu wiadomości elektronicznych oraz ich wymiany (RFC 561 [5], RFC 680 [6], RFC 724 [7], RFC 733 [8]), z których żaden nie został szerzej zastosowany w praktyce.

Jednym z bardziej istotnych kroków w rozwoju poczty elektronicznej były działania podjęte w 1978 r. przez U.S. Army Materiel Command mające na celu stworzenie systemu pozwalającego na transport wiadomości między różnorodnymi systemami. W tym celu stworzony został **M**ulti-purpose **M**emo **D**istribution **F**acility. Jego najważniejszymy cechami była obsługa nie tylko różnorodnych protokołów transportowych poczty elektronicznej, ale także na przykład sieciowych protokołów transportowych, co pozwoliło na integrację w ramach jednej instytucji różnych rozwiązań popularnych w tamtym okresie czasu.

W 1979 r., wraz z wydaniem systemu operacyjnego BSD 4.0, przedstawiony został program `delivermail`, który obsługiwał kolejny stworzony protokół – **U**nix-to-**U**nix **Co**p**y**, choć nie tylko – jedną z większych jego zalet, podobnie jak w przypadku MMDF, była możliwość współpracy z wieloma różnymi protokołami transportowymi jednocześnie. Rozwinięciem tego programu był `sendmail`, który został zaprezentowany wraz z systemem BSD 4.1c w 1983 r. Wraz z rozwojem poczty elektronicznej, rozwijany był również `sendmail`, a jego wysoka sprawność działania spowodowała, iż z czasem stał się on najbardziej popularnym, najpowszechniej używanym w sieci Internet oprogramowaniem służącym do transportu poczty elektronicznej.

Dalszy rozwój rynku usług pocztowych, a szczególnie dalsze zwiększanie się liczby przesyłanych wiadomości, powodowało intensyfikację prac mających na celu stworzenie nowego, bardziej uniwersalnego protokołu wymiany wiadomości. Zostały one uwieńczone powstaniem **S**imple **M**ail **T**ransfer **P**rotocol – w swej pierwszej wersji opublikowanego w RFC 821 [9] w 1982 r. Głównymi założeniami projektowymi tego protokołu, wymienionymi w podanym dokumencie standaryzującym, były prostota, efektywność oraz niezawodność. To właśnie one zagwarantowały sukces SMTP, który widoczny jest do dnia dzisiejszego. Do powodzenia SMTP przyczyniła się także jego implementacja – w niedługim czasie po opublikowaniu specyfikacji, protokół ten obsługiwany był przez oprogramowanie `sendmail`, którego popularność już ówcześnie zataczała coraz szersze kręgi.

2. Protokoły transportu poczty elektronicznej

Współczesny rynek poczty elektronicznej jest praktycznie zmonopolizowany. Przytłaczająca większość ruchu pocztowego realizowana jest za pośrednictwem SMTP. Protokół ten, od swego powstania ponad 25 lat temu, cieszy się niesłabnącą popularnością, dzięki której w chwili obecnej praktycznie nie istnieje na rynku masowym dla niego żadna konkurencja. Na rynkach niszowych, o szczególnych wymaganiach lub szczególnych możliwościach środowiskowych, stosowane jednak wciąż są protokoły, które rozwijały się wcześniej niż SMTP lub równolegle z nim. Najważniejsze z nich to X.400 oraz **U**nix-to-**U**nix **Co**p**y**. Poniżej postaram się podać krótką charakterystykę każdego z trzech wymienionych protokołów, a także przedstawić ich rolę i miej-

sce we współczesnym rynku poczty elektronicznej.

2.1. Simple Mail Transfer Protocol

SMTP, jak sama jego nazwa wskazuje, jest prostym protokołem tekstowym. Jego założenia projektowe uwzględniały co prawda zaawansowane możliwości (np. skomplikowane, przynajmniej jak na początek lat 80. XX. wieku, wyznaczanie marszruty wiadomości), ale stawiały sobie za główny cel prostotę protokołu. Założenie to wynikało z potrzeby posiadania protokołu, który nie tylko spełniałby wymagania nakładane mu przez skomplikowaną strukturę sieci Internet, ale również takiego, który dawałby implementatorom możliwość wdrożenia go w prosty, sprawny sposób – jego autorzy już podczas projektowania protokołu przewidzieli, że jest to najlepszy sposób dla zapewnienia mu sukces.

SMTP, jako protokół projektowany ponad 25 lat temu, z przyczyn oczywistych nie jest przystosowany do zmian, które zachodziły w sieci Internet od czasu jego powstania aż do dziś. Aby więc można go było z powodzeniem stosować we współczesnych czasach, powstało wiele rozszerzeń tego protokołu, które wzbogacają go o nowe możliwości, a także poprawiają, zauważone podczas praktycznego jego stosowania, niedoskonałości. Po prawie 20 latach istnienia protokołu, w 2001 r., najważniejsze z tych rozszerzeń zostały zebrane w jednym dokumencie standaryzującym (RFC 2821 [10]), który wprowadził nową wersję protokołu, znaną popularnie jako **E**xtended **SMTP** (choć oficjalna nazwa pozostała bez zmian).

Najważniejszym, moim zdaniem, z zaprojektowanych rozszerzeń SMTP jest `SMTP AUTH`. Polega ono na dodaniu do protokołu opcjonalnej autoryzacji, dzięki której strona odbiorcza może weryfikować tożsamość strony nadawczej. Przełomowość tego rozszerzenia wiąże się z problemem wysyłania niechcianej poczty przez cudze serwery – aby zapobiec takim praktykom, administratorzy oraz osoby zajmujące się rozwojem SMTP wprowadzili mechanizm, dzięki któremu do danego serwera ma dostęp tylko grupa osób z nim w pewien sposób związanych, tj. jego użytkownicy.

Użytkownicy SMTP od bardzo dawna obawiali się o prywatność prowadzonej przez siebie korespondencji. Mieli do tego bardzo dobre podstawy – w protokole, w którym cała komunikacja przebiega jawnym tekstem, wystarczy proste jej podsłuchanie, aby treść wiadomości przestała być tajemnicą. Problem ten stał się jeszcze poważniejszy i jeszcze bardziej zauważalny w momencie, gdy wprowadzono autoryzację. Rozszerzeniem SMTP, które ma za zadanie naprawić tą niedoskonałość, jest zastosowanie **T**ransport **L**ayer **S**ecurity, najszerzej obecnie stosowanej i uznanej technologii szyfrowania połączeń sieciowych, do bezpiecznego przesyłania danych, które zdefiniowane zostało w RFC 3207 [11].

Warto zauważyć, iż całość ruchu w SMTP jest realizowana w formie komunikacji typu *push*, tzn. strona nadająca inicjuje połączenie w momencie dla siebie dogodnym. Strona odbierająca może co prawda nie przyjąć połączenia w momencie, kiedy jest to dla niej z jakichś względów „niewygodne" (np. zgłaszając błąd tymczasowy w sesji SMTP), jednakże nie ma ona żadnej kontroli nad tym, kiedy strona nadająca ponowi próbę przekazania wiadomości, a nawet czy w ogóle ponowna próba będzie miała miejsce. Od dłuższego czasu taka forma komunikacji jest uważana za znacznie ograniczającą możliwości protokołu, w związku z czym powstało jego rozszerzenie mające na celu zmniejszenie jej konsekwencji, znane jako `ETRN` i zdefiniowane w RFC 1985 [12]. Daje ono odbiorcy wiadomości możliwość zażądania od nadawcy jej doręczenia danym momencie. Jednakże, jak całemu SMTP, również temu rozszerzeniu przyświecała idea prostoty, w konsekwencji czego nie jest to pełna implementacja komunikacji typu *pull*, a jedynie jej drobna namiastka.

Kolejnym istotnym ograniczeniem SMTP w jego pierwotnej formie była możliwość przesyłania jedynie siedmiobitowych znaków z zestawu US-ASCII. Przyczyna nałożenia takiego limitu jest dość oczywista: w czasach, kiedy protokół ten był projektowany, cały rozwój poczty elektronicznej skupiał się w USA, gdzie siedmiobitowe znaki pokrywają cały używany alfabet. Mimo, iż poczta elektroniczna (a w raz z nią także SMTP) szybko dotarła również w inne, nawet najbardziej odległe i najbardziej egzotyczne, zakątki świata, to jednak zestaw znaków siedmiobitowych bardzo długo pozostawał jedynym akceptowanym w SMTP. Użytkownicy oraz autorzy programów z tego protokołu korzystających wymyślili bardzo wiele obejść tego problemu – od najprostszego, jakim jest powstrzymywanie się od używania narodowych znaków diaktrycznych (co jednak jest możliwe jedynie w niektórych językach, których alfabet jest nadzbiorem alfabetu łacińskiego), aż po tak zaawansowane i rozbudowane, jak standard MIME. Wiązały się jednak z nimi kolejne ograniczenia czy niewygodny – np. utrudnione czytanie i komponowanie wiadomości czy też przyrost ich rozmiaru. Ostatecznym rozwiązaniem problemu stało się dopiero wprowadzenie rozszerzenia zwanego `8BITMIME` zdefiniowanego w dokumencie RFC 3030 [13].

2.2. X.400

SMTP to typowy przykład protokołu stworzonego przez środowisko badaczy we wczesnych czasach powstawania globalnej sieci komputerowej. Zupełnie od-

mienne podejście do projektowanego protokołu przedstawione zostało w zestawie rekomendacji definiujących rodzinę protokołów X.400 [14]. Stanowią one wynik wspólnej pracy organizacji ITU-T oraz ISO, a zatem są dziełem zespołu fachowców, którzy dążyli do zaprojektowania kompletnego, rozbudowanego, dobrze przetestowanego systemu wymiany elektronicznych wiadomości pocztowych. Cel ten został osiągnięty w pełni: powstała rodzina standardów, która definiuje praktycznie każdy możliwy aspekt związany z pocztą elektroniczną – od jej transportu, poprzez wyznaczanie marszruty wiadomości, aż po kształt samych wiadomości i ich przechowywanie. Stworzone w ten sposób rozwiązania kładą nacisk na kompletność i bezpieczeństwo powstałego protokołu, a co za tym idzie – możliwość wykorzystania go w bardzo wielu specyficznych zastosowaniach, w których protokół o rozbudowanych możliwościach jest niezbędny. Najbardziej znanym przykładem demonstrującym rozbudowanie X.400 jest zastosowany w nim schemat adresowania. Został on opracowany w sposób tak rozbudowany i uniwersalny, iż stał się z czasem odrębnym standardem nazwanym X.500 i służącym budowaniu bardzo skomplikowanych usług katalogowych. Współcześnie rozwiązanie pochodne od X.500 jest bardzo szeroko wykorzystywane i znane jako **L**ightweight **D**irectory **A**access **P**rotocol.

Pozornie rodzina protokołów X.400 nie jest popularna we współczesnym rynku usług związanych z transportem poczty elektronicznej. Jest to jednak dość mylne wrażenie, wynikające z ograniczonych możliwości badania tych niszy rynkowych, dla których X.400 jest podstawowym sposobem wymiany elektronicznych wiadomości pocztowych. Chodzi tu mianowicie o sieci wewnętrzne dużych organizacji – dużych korporacji, wojska, lotnictwa, marynarki itp., gdzie jego zalety są szeroko doceniane, a nierzadko jest również tworzone oprogramowanie specjalizowane do jego obsługi.

2.3. Unix-to-Unix CoPy

W odróżnieniu od opisanych wcześniej STMP i X.400, protokół UUCP nie był projektowany z myślą o transporcie poczty elektronicznej. Jego pierwotne przeznaczenie było bardziej ogólne: miał on służyć do szeroko pojętego zdalnego wykonywania komend oraz przesyłania plików między komputerami działającymi pod kontrolą uniksowego systemu operacyjnego. Z czasem jednak stał się on pierwszym w tym środowisku szeroko uznanym protokołem transportu poczty elektronicznej – takie jego zastosowanie zostało ustandaryzowane w RFC 976 [15].

UUCP, jako protokół projektowany do współpracy z niezbyt stabilnymi i niepewnymi z natury łączami telefonicznymi, posiada szerokie możliwości poprawiania niezawodności przesyłania danych. Do najważniejszych z nich należą automatyczny wybór zapasowego sposób przesłania danych w momencie, gdy podstawowy zawiedzie czy też automatyczne zestawianie połączeń z systemami, do których przesyłanie danych jest w danej chwili niezbędne. Również format danych wymienianych w protokole w widoczny sposób zaprojektowany jest do współpracy z łączami telefonicznymi o niewielkiej prędkości. Ilości informacji przesyłanych między komunikującymi się systemami są możliwie jak najmniejsze, co pierwotnie miało służyć uzyskaniu jak największej prędkości przesyłania danych, z czasem zaś zaczęło być postrzegane również jako czynnik zwiększający niezawodność transmisji w protokole UUCP.

Protokół UUCP wprowadził kilka rozwiązań technicznych, które w późniejszym okresie stały się bardzo popularne w innych, zupełnie z nim nie powiązanych zastosowaniach. Najważniejszym z nich jest schemat adresowania wiadomości. W UUCP miał on postać „`host!user`”. Znak „`!`” został przejęty przez twórców SMTP i obecnie jest w nim wykorzystywany do wyznaczania marszrut wiadomości explicite przez jej nadawcę. Notacja ta jest stosowana również w protokole NNTP, w którym służy ona do przedstawiania trasy, którą wiadomość przebyła w drodze od nadawcy do serwera, z którego pobrał ją odbiorca.

W chwili obecnej protokół UUCP wykorzystywany jest jedynie w bardzo specyficznych niszach rynkowych, w których jego zalety są zdecydowanie istotniejsze od licznych wad, które posiada. Pierwszym polem zastosowania, w którym bardzo chętnie jest on stosowany jest komunikacja poprzez łącza telefoniczne o bardzo wysokim koszcie połączenia – na przykład satelitarne łącza dla cywilnej floty morskiej. Drugą znaczącą niszą, w której UUCP znalazł zastosowanie są korporacyjne łącza między oddziałami, dla których wymagana jest najwyższa niezawodność z praktycznie stałą dostępnością. Korzysta się przy implementacji takich połączeń z protokołu UUCP dzięki jego możliwościom wyboru alternatywnego sposobu połączenia w przypadku, gdy podstawowy sposób zawodzi. Zazwyczaj stosowaną kombinacją jest transport danych protokołu UUCP poprzez łącza TCP sieci Internet w wersji podstawowej z opcją przełączenia się na alternatywną komunikację po łączach telefonicznych.

3. Znane problemy

Współczesny rynek poczty elektronicznej jest bardzo silnie rozwinięty i dostęp do usług z nią związanych jest bardzo szeroko rozpowszechniony. Powszechny dostęp do poczty elektronicznej oznacza w szczególności również bezproblemowe z niej korzystanie przez osoby, które nie mają na celu jedynie komunikacji z inny-

mi jej użytkownikami, a przynajmniej nie w powszechnie uznanym tego sformułowania znaczeniu. Podczas rozwoju poczty elektronicznej dało się zaobserwować tendencję, która zdaje się być naturalna i zauważalna w większości dziedzin aktywności ludzkiej: część osób postanowiła skorzystać z możliwości, jakie wymiana elektronicznych wiadomości pocztowych daje, dla własnych, egoistycznych celów, mniej lub bardziej celowo kosztem innych jej użytkowników. Wpływ takich działań na kształt poczty elektronicznej z czasem się nasilał, gdyż wraz z rozwojem omawianego rynku, rosła proporcjonalnie również liczba pojawiających się na nim nadużyć. Ich rozwój w pewien sposób ułatwiło również samo środowisko osób związanych z tworzeniem i rozwojem usług pocztowych w przeszłości, które początkowo charakteryzowało się dużą otwartościąi ufnością. Cecha ta została szybko zauważona przez osoby o zamiarach niezbyt godnych pochwały i bardzo skrzętnie przez nich wykorzystana. Środowisko co prawda potrafiło się bardzo szybko przystosować i otwartość zamieniono na ochronę przed nadużyciami, jednak trend wykorzystywania poczty elektronicznej w sposób, którego pierwotnie nikt nie planował, pozostał i ma wielu przedstawicieli aż po dzień dzisiejszy. Inną przyczyną wykorzystywania poczty elektronicznej do nagannych celów jest możliwość czerpania z niej komercyjnych, wymiernych korzyści. W momencie, kiedy poczta elektroniczna zaczęła dawać możliwość zarobku (bezpośredniego lub pośredniego), pojawiły się osoby, które czerpane z niej zyski chciały zmaksymalizować za wszelką cenę. Zachęcała ich do tego tym bardziej bezpłatność i powszechna dostępność tego medium komunikacji, czyli bardzo niskie koszty do uzyskania zamierzonych korzyści prowadzące. Rynek poczty elektronicznej został zatem zaatakowanych przez marketingowców i „specjalistów" od reklamy, którzy gotowi byli zrobić wszystko, aby dotrzeć do jak najszerszego grona odbiorców, włącznie z łamaniem podstawowych zasad w sieci Internet obowiązujących. Nie zyskali oni sympatii wśród pozostałych użytkowników poczty elektronicznej ani wśród administratorów serwerów pocztowych i zaczęli być obraźliwie nazywani „*marketoidami*".

Jednym z najbardziej widocznych i najbardziej dokuczliwych negatywnych zjawisk występujących na współczesnym rynku poczty elektronicznej jest *spam*. Nie istnieje jego jednoznaczna definicja – być może ze względu na duży stopień skompilowania tego zjawiska, czy też może ze względu na jego różny odbiór przez różnych użytkowników poczty elektronicznej. Dla potrzeb niniejszego artykułu chciałbym zaproponować następującą definicję roboczą:
Spam — masowo rozsyłana korespondencja, której odbiorca nie zamawiał ani która nie jest skierowana do niego osobiście
Jestem jednak świadom, iż definicja ta nie jest pełna ani uniwersalna. Praktycznie jedyną kwestią, w której wszyscy użytkownicy poczty elektronicznej definiując spam są zgodni, jest fakt, iż nazywać w ten sposób należy wiadomości, których odbiorca nie życzył sobie otrzymać. Jednak już w tym momencie należy zastanowić się, czy ten element definicji jest taki oczywisty, jak się wydaje. Moja definicja zawiera dodatkową klauzulę, która stanowi zabezpieczenie przed nazywaniem spamem wiadomości, które są wyraźnie adresowane do odbiorcy i zawierają specyficzną dla niego treść, jednakże z pewnych względów nie przypadły mu do gustu. Pierwszym aspektem podanej przeze mnie definicji, który może być dyskusyjny, jest masowość rozsyłanej korespondencji. Główną wątpliwością, która pojawia się w tym momencie, jest wyznaczenie wartości granicznej, przy której rozsyłaną pocztę uznaje się za masową. Oczywiście nie istnieje uniwersalna wartość progowa, decyzję o masowości należy podejmować odrębnie dla każdego przypadku, co sprawia, iż jest to bardzo subiektywne kryterium. Inną kwestią, często podnoszoną przy definiowaniu spamu, jest chęć przez niektórych ograniczenia tej definicji tylko do wiadomości o charakterze komercyjnym, czyli głównie różnego rodzaju reklam. Takie ograniczenie zostało wprowadzone w polskim prawodawstwie w Ustawie o Świadczeniu Usług Drogą Elektroniczną. Miała ona pierwotnie wprowadzić podstawy prawne do karania osób rozsyłających spam, jednakże przewiduje jedynie kary (nota bene bardzo niskie) dla osób rozsyłających Niezamówioną Informację Handlową, która, w oczywisty sposób, nie jest tym samym, co spam. Subiektywność, która jest widoczna podczas tworzenia definicji spamu, przez niektórych włączana jest do tej definicji jako główny jej składnik. Twierdzą oni, iż spam to „*każda korespondencja, którą odbiorca uzna za spam*". Moim zdaniem taka definicja jest nieuprawniona, gdyż pozwala na wiele nadużyć, przed którymi w mojej definicji zabezpieczenie stanowi ostatnia jej część.

Niechciane wiadomości na współczesnym rynku poczty elektronicznej stanowią przytłaczającą większość ruchu pocztowego w sieci Internet. Podanie konkretnej statystyki dotyczącej odsetku wiadomości uznawanych za spam jest dosyć trudne. Dane dostępne w różnych źródłach twierdzą, iż jest to od około 70% aż do ponad 95%. Przyczyną tak wielkiego rozrzutu między podawanymi statystykami jest, moim zdaniem, duży kłopot z opracowaniem spójnej i z dużym prawdopodobieństwem poprawnej metodyki służącej prowadzeniu badań nad skalą zjawiska spamu. Według mnie najbardziej wiarygodnymi danymi są te, które zbierane

są przez same serwery pocztowe z tym zjawiskiem walczące. Jedno z ich źródeł, projekt Distributed Checksum Clearinghouse, podaje statystyki [16] zbliżające się właśnie do 70%. Wielkość ta oznacza ok. 300 000 000 niechcianych wiadomości, które każdego dnia trafiają do skrzynek pocztowych użytkowników sieci Internet. Dla statystycznego użytkownika poczty elektronicznej oznacza to próbę doręczenia do niego blisko czterystu wiadomości, których otrzymania by on sobie nie życzył. Liczba ta jest efektem rozpowszechnienia poczty elektronicznej we współczesnym świecie – podczas jej rozwoju, ilość niechcianych wiadomości rosła praktycznie liniowo wraz ze wzrostem ogólnego ruchu pocztowego. Współcześnie obserwuje się swego rodzaju nasycenie rynku spamu – mimo dalszego wzrostu ogólnej liczby przesyłanych wiadomości poczty elektronicznej, wolumin spamu od pewnego czasu pozostaje na w przybliżeniu stałym poziomie. Jeżeli taka tendencja utrzyma się, to być może można traktować ją jako zapowiedź zmniejszenia znaczenia problemu spamu w przyszłości. Istotnym kłopotem, z którym borykają się osoby badające zjawisko niechcianej poczty elektronicznej, jest fakt jego wykrywalności. Wszelkie statystyki mogą być tworzone tylko pod warunkiem istnienia skutecznych metod pozwalających wyrywać spam, tzn. skutecznie odróżniać go od pozostałej części ruchu pocztowego. W chwili obecnej jednak nie istnieją metody skuteczne w 100%, choć skuteczność wykorzystywanych metod jest bardzo wysoka. Średnio serwery pocztowe potrafią ponad 90% niechcianych wiadomości pocztowych wykryć, a istnieją nawet metody (choćby opisane w [17]) zwiększające ten odsetek aż do poziomu 99.85%.

Innym, nie mniej poważnym, choć o wiele rzadziej zauważanym problemem, który obecny jest na współczesnym rynku usług związanych z pocztą elektroniczną, jest zagadnienie możliwości identyfikacji nadawcy wiadomości. Chodzi tutaj o identyfikację osoby, firmy czy też instytucji, która wysłała daną wiadomość, na przykład w celu ułatwienia weryfikacji autentyczności informacji w niej zawartych.Pierwszym, bardzo istotnym zagrożeniem, przed którym stajemy w sytuacji, w związku z tym problemem, jest możliwość oszustwa – sfałszowania informacji adresowych i podpisu wiadomości tak, aby wyglądała ona na nadaną przez kogoś innego. Najwięcej fałszerstw informacji adresowych zawartych w wiadomościach poczty elektronicznej służy oszustwom mającym konsekwencje finansowe. Chodzi tu przede wszystkim o wyłudzenia różnego rodzaju danych identyfikacyjnych pozwalające następnie przestępcom na uzyskanie dostępu na przykład do konta bankowego czy karty płatniczej ofiary. Proceder taki nazywany jest *phishing*. Warto zauważyć, iż problem ten bezpośrednio łączy się z problemem rozsyłania niechcianej korespondencji. Po pierwsze korespondencja mająca na celu wyłudzenie pieniędzy nie może być uznana za pożądaną, a po drugie techniki rozsyłania takich wiadomości są identyczne, jak techniki rozsyłania spamu. Możliwości sfałszowania danych sugerujących tożsamość nadawcy wiadomości w połączeniu z technikami spamerskimi są wykorzystywane także w działaniach nieuczciwej konkurencji między firmami. Mianowicie firma, która chce zaszkodzić swojej konkurencji, rozsyła dużą liczbę niechcianych wiadomości, które identyfikowane są danymi firmy konkurencyjnej, a najczęściej również wprost reklamują jej produkty. Wykorzystana tutaj zostaje powszechna niechęć do spammerów, która pozwala oczernić konkurencję, a co za tym idzie – być może niewielkim kosztem przejąć część z jej zysków. Jednakże fałszowanie danych nadawcy wiadomości może stanowić dla ofiar takiej działalności zagrożenie nie tylko z finansowego punktu widzenia. Proceder tak zwanej „kradzieży tożsamości" może mieć również ogromne znaczenie w sensie społecznym. Nie stanowi bowiem problemu stworzenie wiadomości o zmienionych danych nadawcy, której treść będzie następnie wykorzystana w celu zdyskredytowania w pewien sposób osoby, pod którą nadawca się podszywa. Nie prowadzi go to co prawda do uzyskania korzyści materialnych, jednak może zapewnić mu zyski na polu na przykład towarzyskim, które niejednokrotnie mogą być o wiele cenniejsze.

Przedstawione powyżej zagadnienia nie są oczywiście jedynymi problemami, z którymi boryka się współczesny rynek poczty elektronicznej. Istnieje jednak wiele dalszych problemów, z którymi boryka się opisywany rynek, jednakże większosc z nich dotyka głównie osób zajmujących się stroną administracyjną, organizacyjną czy też rozwojem oprogramowania służącego do obsługi poczty elektronicznej. Najbardziej zauważalnymi wśród nich problemów są kłopoty z wyznaczaniem marszruty wiadomości, a także, co jest z poprzednim powiązane, efektywnym ich adresowaniem. Równie problematyczny jest fakt praktycznego braku obsługi załączników w protokole SMTP – muszą one być w chwili obecnej przesyłane jako integralne części wiadomości, co nie jest rozwiązaniem wygodnym ani funkcjonalnym. Istnieją również inne, pomniejsze problemy, których przyczyną są cechy współczesnego rynku usług pocztowych i wykorzystywanych na nim protokołów, jednakże są one albo lokalne dla pewnych środowisk, albo występują jedynie w specyficznych sytuacjach.

4. Podsumowanie

Opisana sytuacja panująca na współczesnym rynku poczty elektronicznej nie przedstawia się zbyt optymistycznie. Mimo tego, popularność usług z nim związa-

nych nie tylko nie spada, ale wręcz cały czas rośnie. Związane jest to z bardzo wieloma sposobami eliminacji skutków problemów widocznych podczas przesyłania elektronicznych wiadomości pocztowych. Istnieją współcześnie bardzo rozbudowane systemy pozwalające ograniczać ilość spamu docierającego do użytkowników końcowych poczty elektronicznej. Również problem identyfikacji rzeczywistego nadawcy wiadomości jest ograniczany poprzez stosowanie różnych metod pozwalających na uwierzytelnianie go z mniejszą lub większą pewnością. Jednakże wszystkie stosowane w tym celu rozwiązania mają wspólną wadę: nie są rozwiązaniami systemowymi mającymi na celu eliminację przyczyn tych zjawisk i uniemożliwienie ich występowania w przyszłości, a jedynie sposobami na „łatanie" i minimalizowanie widocznych skutków tych zjawisk. Moim zdaniem nie jest to właściwe podejście do problemu, gdyż w perspektywie czasowej tworzenie tego typu rozwiązań musi w pewnym momencie stać się nieopłacalne lub wręcz niewykonalne technicznie. Skoro więc ewolucyjna zmiana sytuacji związanej współcześnie z transportem poczty elektronicznej w sieciach komputerowych okazuje się podejściem nieodpowiednim, zaproponować chciałbym zupełnie inne podejście – rewolucyjne. Moja propozycja polega na stworzeniu nowego protokołu transportu poczty elektronicznej, który już w założeniach projektowych wolny byłby od głównych wad protokołów wykorzystywanych w chwili obecnej. Szczegóły tego rozwiązania, a także praktyczna jego implementacja, wykracza poza zakres tematyczny niniejszego artykułu i stanowi treść mojej pracy magisterskiej, a w przyszłości – również rozprawy doktorskiej.

Bibliografia

[1] Tom Van Vleck. *The History of Electronic Mail*. `http://www.multicians.org/thvv/mail-history.html`.

[2] Ray Tomlinson. *The First Network Email*. `http://openmap.bbn.com/~tomlinso/ray/firstemailframe.html`.

[3] *RFC 2822: Internet Message Format*. 2001.

[4] *RFC 354: The File Transfer Protocol*. 1972.

[5] *RFC 561: Standardizing Network Mail Headers*. 1973.

[6] *RFC 680: Message Transmission Protocol*. 1975.

[7] *RFC 724: Proposed Official Standard for the Format of ARPA Network Messages*. 1977.

[8] *RFC 733: Standard for the Format of ARPA Network Text Messages*. 1977.

[9] *RFC 821: Simple Mail Transfer Protocol*. 1982.

[10] *RFC 2821: Simple Mail Transfer Protocol*. 2001.

[11] *RFC 3207: SMTP Service Extension for Secure SMTP over Transport Layer Security*. 2002.

[12] *RFC 1985: SMTP Service Extension for Remote Message Queue Starting*. 1996.

[13] *RFC 3030: SMTP Service Extensions for Transmission of Large and Binary MIME Messages*. 1996.

[14] *ITU-T Reccomendation X.400/F.400 (ISO/IEC 10021) Data Communication Networks for Message Handling Systems*. 1999.

[15] *RFC 976: UUCP Mail Interchange Format Standard*. 1986.

[16] Distributed Checksum Clearinghouse. *Distributed Checksum Clearinghouse Graphs*. `http://www.dcc-servers.net/dcc/graphs/?resol=5y&BIG=1`.

[17] Jonathan A. Zdziarski. *Ending Spam. Bayesian Content Filtering and the Art of Statistical Language Classification*. No Starch Press, 2005.