

**АНАЛИЗ ОСОБЕННОСТЕЙ ПОСТРОЕНИЯ СИСТЕМЫ ЭЛЕКТРОННОЙ  
ПОЧТЫ X.400 НА ОСНОВЕ ЗАЩИЩЕННОЙ TCP/IP СЕТИ  
Ежов А.В. Email: Ezhov1134@scientifictext.ru**

*Ежов Алексей Викторович – соискатель ученой степени кандидат технических наук,  
кафедра систем связи и телекоммуникаций,  
филиал Военной Академии, г. Серпухов*

**Аннотация:** в последние годы популярность электронной почты быстро растет и по некоторым оценкам ее сегодня использует около ста миллионов человек в мире, а число ее клиентов в России превысило 500 тысяч человек. Один из идеологов Internet У. Серф (W.Serf) отмечал, что в Internet никто ничего не может реально гарантировать. Применение защищённых сетей обмена данными становится всё более актуальным как для отдельных граждан, так и для организаций различного типа. Системы X.400 / X.500 находятся на службе у большинства известных провайдеров телекоммуникационных услуг и являются наиболее привлекательной технологической платформой для построения систем обмена электронными сообщениями многих крупных коммерческих компаний в США и Европе.

**Ключевые слова:** адрес, аппаратура, информация, криптографическая защита, накопление, обработка, передача электронных сообщений, протокол, система, сети обмена данными, уровни, X.400.

**THE ANALYSIS OF FEATURES OF CREATION OF SYSTEM OF E-MAIL X.400  
ON THE BASIS OF THE PROTECTED TCP/IP OF THE NETWORK  
Ezhov A.V.**

*Ezhov Alexey Viktorovich – applicant of an academic degree Candidate of Technical Sciences,  
DEPARTMENT OF COMMUNICATION SYSTEMS AND TELECOMMUNICATIONS,  
BRANCH OF MILITARY ACADEMY, SERPUKHOV*

**Abstract:** in recent years popularity of e-mail quickly grows and by some estimates it is used today by about hundred million people in a pattern, and the number of her clients in Russia exceeded 500 thousand people. One of ideologists of Internet U. W.Serf marked that in Internet nobody can really guarantee anything. Application of the protected networks of a data interchange to become more and more urgent both for certain citizens, and for the organizations of different type. Systems X.400/X.500 are on service of most the known providers of telecommunication services and are the most attractive technological framework for creation of systems of exchange of electronic messages of many large business firms in the USA and Europe.

**Keywords:** address, equipment, information, cryptography protection, accumulation, processing, transmission of electronic messages, protocol, system, data interchange networks, levels, X.400.

УДК 621.3

Криптографической основой защищенной сети обмена данными (ЗСОД) является аппаратура передачи данных (АПД), которая предназначена для гарантированного шифрования, имитозащиты, распределения, приема и передачи данных по каналам связи в дуплексном и симплексном режимах [1].

Аппаратура криптографической защиты (АКЗ) должна обеспечивать:

- автоматическую помехозащищенную передачу и прием по каналам связи смешанной СПД информационных пакетов, передачу управляющей информации в специальном формате и режиме;
- работу по обходным маршрутам, автоматическую защиту от размножения и заикливания сообщений;
- передачу сообщений категорий срочности при использовании дисциплины обслуживания с относительным приоритетом;
- автоматизированную передачу одноадресных сообщений, многоадресных сообщений группе абонентов, циркулярных сообщений группам абонентов;
- маскирование трафика с выравниванием длин канальных кадров и интервалов между ними;
- жесткое администрирование топологии сети (статическое планирование сетевой конфигурации);
- иметь возможность наращивания канальной емкости;
- работать с ЭВМ по интерфейсу Ethernet.

Исходя из изложенного, особенностями построения ЗСОД на базе АКЗ являются [5]:

- 1) использование динамических методов маршрутизации трудно реализуемо вследствие директивного статического планирования сетевой конфигурации;
- 2) канальный трафик представляет собой синхронную последовательность коротких кадров, в которую в целях маскирования включаются «пустые» кодограммы;

3) IP пакеты длиной более кадра фрагментируются, причем получающиеся при этом «неполные» фрагменты дополняются нулевым («пустым») содержимым.

Кроме того, возможно применение технологий на базе протокола X.400. Система электронной почты (СЭП), базирующаяся на рекомендациях X.400 – реальная и наиболее полная реализация многоуровневой модели взаимодействия открытых систем (ВОС). Модель ВОС позволила не только создавать глобальные полностью распределенные системы передачи данных, но и обеспечить их взаимодействие на разных уровнях по стандартным интерфейсам и общим правилам. Так называемый, физический, или самый нижний уровень модели, унифицирует физические (электрические) интерфейсы. Канальный уровень – унифицирует разного рода каналы связи, включая физические (медные), микроволновые, радио, оптоволоконные, спутниковые и прочие [2].

Сетевой и частично транспортный уровни позволяют создавать различные сети передачи данных (СПД) с протоколами X.25, TCP/IP (Интернет), Frame Relay и другие. Точно так же, как СПД опираются на кабельные и канальные системы, X.400 использует данные сети в качестве собственной инфраструктуры. Можно сказать, что в модели ВОС все уровни X.400 лежат выше сетей передачи данных. В отличие от СПД системы X.400 оперируют не данными как абстрактной единицей информации, а сообщениями, т.е. неким законченным объемом информации в виде текста, графики, речи, изображения и прочие. При этом допускается различное преобразование сообщений из одного вида в другой [3].

В настоящее время существует множество различных СЭП, однако только две из них завоевали всемирное признание в качестве глобальных систем. Первая СЭП – это широко известная электронная почта Internet. Вторая – система X.400, отличающаяся от первой высокой надежностью и расширенным сервисом. Указанные два типа электронной почты дополняют друг друга. Поэтому в достаточно крупных организациях используются системы обоих типов: Internet системы используют для связи с внешним миром, системы X.400 применяют для организации безупречной службы корпоративного документооборота [2].

Современные системы на базе X.400 позволяют обходиться без специальных Internet систем, поскольку они поддерживают протоколы SMTP/POP3. С другой стороны, развитие Internet систем электронной почты идет в направлении приближения к возможностям X.400: вводятся такие услуги как извещения и различные типы содержимого сообщений.

Первоначально стек протоколов X.400 строился с учетом использования первых трех уровней модели OSI (физического, канального и сетевого), которые в то время реализовывались исключительно с помощью протоколов X.25. Дальнейшее развитие сетевых технологий привело к использованию различных стандартов локальных сетей, а также TCP/IP в качестве протоколов нижних уровней систем на базе X.400.

В спецификациях стандарта X.400 основное внимание уделяется обеспечению широкого набора услуг и надежной передачи сообщений. Таких услуг в X.400 не один десяток. Тем не менее, практика показала, что наиболее важными из них являются уведомление отправителя о доставке и прочтении сообщения. Наличие таких услуг переводит электронную почту из любительского средства обмена сообщениями в службу документированного делового документооборота, отвечающего самым жестким современным требованиям.

В рекомендации X.400 заложены возможности сопряжения служб на базе этого протокола с другими почтовыми системами и телематическими средами, в частности, системами электронного обмена факсимильными, телексными и телеграфными сообщениями, а также данными разного типа (двоичные, голос, видео) [1].

Использование рекомендаций серии X.400 практически исключает возможность потерь или искажений при передаче информации. Отчасти это объясняется тем, что они, в отличие от электронной почты Internet, изначально разрабатывались для коммерческих целей, а одним из главных требований была высокая надежность передачи сообщений.

Рекомендации X.400 являются единственным признанным на международном уровне промышленным стандартом передачи электронных сообщений. Протокол X.400 поддерживается всеми ведущими производителями программного обеспечения. Широкое использование этого протокола в глобальных и национальных общедоступных сетях, в том числе разработчиками систем автоматизированного документооборота, позволяет осуществлять прозрачный обмен сообщениями [2].

При передаче сообщений в стандарте X.400 отсутствуют проблемы, свойственные другим технологиям (незащищенность доступа к информации абонентов, ненадежность обмена сообщениями, проблемы перекодировки пересылаемой информации и др.). Эта идиллическая картина резко отличается от передачи сообщений электронной почты в Internet.

Системы и службы обработки сообщений дают возможность пользователям обмениваться сообщениями на основе их передачи и промежуточного накопления. Сообщение, подготовленное одним

пользователем-отправителем, передается системой передачи сообщений (СПС) – основным компонентом СОС и затем доставляется одному или нескольким пользователям-получателям сообщений.

СОС содержит различные взаимосвязанные функциональные объекты. Агенты передачи сообщений (АПС) взаимодействуют для выполнения функций передачи сообщений с промежуточным накоплением. Хранилища сообщений (ХС) позволяют хранить сообщения и обеспечивают их предоставление, поиск и управление. Агенты пользователя (АП) помогают пользователям осуществлять доступ к СОС. Модули доступа (МД) обеспечивают связи с другими системами предоставления услуг и службами различных видов, например, с другими телематическими службами, почтовыми службами.

Система обработки сообщений (СОС) – модель, описывающая технологические и организационные процессы, связанные с подготовкой, передачей, обработкой и приемом сообщений.

Пользователь – физическое лицо, либо вычислительный процесс. Пользователи подразделяются на непосредственно взаимодействующих с СОС, и косвенных, взаимодействующих с СОС через другие телематические службы.

Отправитель – пользователь, отправляющий сообщения.

Получатель – пользователь, принимающий сообщения.

Хранилище сообщений – компонент СОС, обеспечивающий одного пользователя возможностями хранения сообщений.

Агент передачи сообщений – функциональный объект, фактически переносящий информационные объекты к пользователям и в списки распределения.

Система передачи сообщений – функциональный объект, содержащий один или несколько агентов передачи сообщений и обеспечивающий передачу сообщений с промежуточным накоплением между агентами пользователя, хранилищами сообщений и модулями доступа.

Агент пользователя (АП) – прикладной процесс, взаимодействующий или с СПС или с хранилищем сообщений для предоставления сообщений от имени одного пользователя. СПС охватывает большое число АПС, которые взаимодействуют по методу передачи сообщений с промежуточным накоплением.

Сообщение состоит из конверта и содержимого. Конверт содержит информацию, используемую СПС при передаче сообщения внутри СПС. Содержимое – это порция информации, которую АП отправителя желает доставить одному или нескольким АП получателям. СПС не изменяет и не анализирует содержимое за исключением операций преобразования. Содержимое сообщения СПС является базовым сообщением и может содержать внутри себя конверт межперсонального сообщения (МП) и содержимое межперсонального сообщения, которое состоит из заголовка и тела, содержащего части тела.

Тело сообщения – информационный объект, непосредственно переданный отправителем и полученный получателем.

В системах X.400 понятие адреса относится не только к отправителю-получателю, но и к списку распределения (СР), или листу рассылки. Каждый отправитель-получатель и СР должен иметь не менее одного адреса, отличающего его от других и определяющий точку его местоположения.

Адреса отправителей-получателей X.400 формируются в соответствии с рекомендациями МСЭ серии X.400 и могут содержать следующие поля (атрибуты) [4]:

<C = > (Country) - код страны. Он состоит из двух латинских букв (RU – Россия, FR – Франция и т.д.), например C = RU;

<ADMD = >(ADministrative Management Domain) – имя административной области управления, например, ADMD = Military\_Institute;

<PRMD = >(PRivate Management Domain) – имя частной области управления, например PRMD = IAS;

<O = >(Organization) – название организации, например O=TOPOL;

<OU = >(Organization Unit) – название подразделения в организации, например OU = OAUNI;

<S = > (Surname) – фамилия абонента, например S = IVANOV;

<G = > (Given name) – имя абонента, например G = ANTON;

<I = > (Initials) - инициалы абонента, например I = SI.

Возможны также другие атрибуты.

В зависимости от типа терминала, с которого абонент взаимодействует с СОС, адрес может задаваться в следующих формах: мнемонической, цифровой, почтовой и терминальной.

Любой отправитель-получатель системы X.400 должен иметь возможность отправить сообщение по адресам следующих типов в зависимости от телематической среды, в которой работают получатели его сообщений:

- адрес в формате X.400;
- факсимильный адрес;
- телексный адрес, адрес абонента сети;
- адрес абонента телеграфной сети общего пользования;
- адрес абонента системы X.400, представленный цифровым номером;
- адрес в формате, используемый в Internet;

- физический адрес для системы бумажной почты.

При отправке сообщений абонентам электронной почты, имеющим адрес в формате Internet, должны выполняться преобразования адресов в соответствии с правилами, изложенными в рекомендациях RFC1327.

Для автоматической рассылки корреспонденции по спискам адресов в X.400 должен быть реализован механизм листов рассылки. Администратор может зарегистрировать для абонента X.400 лист рассылки, который представляет собой некоторый адрес, не являющийся адресом реального абонента в системе. Этому адресу – листу рассылки – ставится в соответствие один или несколько адресов реальных получателей различного типа.

В конверте сообщения физической доставки указываются служебные реквизиты и почтовый адрес получателя. Адрес указывается в стандарте X.400 и представляет собой набор полей с заданными значениями.

В АП отправителя-получателя должен быть предусмотрен механизм адресной книги, позволяющей автоматически заменять любые мнемонические адреса, введенные пользователем их эквивалентным адресом X.400, например, имя «АДЭ» может обозначать список адресов, включая адреса X.400, факсимильные, телексные, адреса физической доставки и прочие.

Качество предоставления услуг может быть охарактеризовано следующими показателями:

технологическими:

- гарантированным временем доставки сообщения;
- доступностью подключения к сети X.400;
- полным соответствием перечню базовых (обязательных) услуг (см. выше);
- количеством дополнительных услуг;
- наличием и количеством соединений (шлюзов) с другими системами телематических служб;
- наличием средств защиты от несанкционированного доступа;
- возможностью отправки-приема сообщений в/из сети Internet.

административными:

- обеспечением бесперебойного круглосуточного функционирования системы;
- количеством юридически значимых соглашений по установлению соединений с другими областями административного управления, в первую очередь со всеми российскими;
- количеством частных регионов управления.

Исходя из изложенного, системы X.400 предназначены, прежде всего, для защищенного и надежного документооборота. В таких системах гарантируется не только сама доставка, но и определенный срок доставки сообщений. Извещения о доставке, прочтении сообщения или о его недоставке – фундаментальные атрибуты технологии электронной переписки X.400. Именно поэтому системы на базе X.400 используются там, где высоки требования к достоверности, надежности и защищенности информации – в банковских структурах, корпоративных сетях, государственных структурах (Министерство обороны, таможенная служба, налоговая инспекция, казначейство и т.д.), а также для телеграфной связи.

Электронные почтамты на базе X.400 идеально приспособлены для крупных территориально распределенных организаций, поскольку обеспечивают гибкую маршрутизацию, надежную, оперативную и защищенную доставку сообщений любого типа (текстовых и факсимильных, телеграмм и телексов, графических и голосовых), администрирование всей сети, а также получение полной статистики почтового обмена.

Развитие сетей X.400 происходит в тесном взаимодействии с Ассоциацией по электронным сообщениям (Electronic Messaging Organization) и ее европейским подразделением – European Electronic Messaging Association, которые регулярно публикуют таблицы установленных соединений систем электронной почты на базе X.400. В Российской Федерации работы по созданию нормативной базы в данной области координируются Ассоциацией документальной электросвязи (АДЭ), при которой существует комитет «Сети X.400».

#### *Список литературы / References*

1. *Манн С.* Linux. Администрирование сетей TCP/IP. Второе издание. Пер. с англ.: Скотт Манн, Митчелл Крелл. М.: Бином-Пресс, 2008. 672 с.
2. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2012. 944 с.
3. *Фрэнк Г., Фриш И.* Сети, связь и потоки. М.: Связь, 1978. 447 с.
4. *Орехов С.Е., Сысоев И.В.* Оптимизация распределения TCP нагрузки по параллельному сетевому тракту сети связи с многомерной маршрутизацией пакетов. Известия Института инженерной физики, 2014. № 1 (31). С. 57-59.

5. *Ежов А.В.* Натурное моделирование процесса многомерной маршрутизации пакетов в TCP/IP сети. Вестник науки и образования, 2017. № 2 (26). С. 19-24.