МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ДЕПАРТАМЕНТ НАУЧНО-ТЕХНОЛОГИЧЕСКОЙ ПОЛИТИКИ
И ОБРАЗОВАНИЯ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«КРАСНОЯРСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

Шифрование информации с помощью криптографической системы PGP за 8 дней

Красноярск
2018

Шифрование информации с помощью криптографической системы PGP за 8 дней: [Текст]: учебное пособие / сост.: Миндалёв И.В. -- Красноярск, Краснояр. гос. аграр. ун-т., 2018, 110 с.

Учебное пособие представляет собой практическое руководство по использованию популярной криптографической системы Pretty Good Privacy (PGP) в шифровании с открытым ключом для защиты данных и электронной почты. Пособие содержит описание методов криптографии в объеме, необходимом для практической работы. На конкретном примере рассмотрен порядок установки PGP на персональном компьютере, применение PGP по шифрованию и расшифровке информации, по цифровой подписи документов.

Предназначено для студентов, изучающих дисциплины «Информационная безопасность», «Правовая защита интеллектуальной собственности» по направлению 09.03.03 «Прикладная информатика», «Криптографические методы защиты информации» по направление 01.03.02 Прикладная математика и информатика.

Рецензенты: Н. Н. Воробович, д-р. техн. наук, проф. СибГТУ; С. И. Сенашов, д-р. физ.-мат. наук, проф. КГТЭИ.

Печатается по решению редакционно-издательского совета Красноярского государственного аграрного университета

Введение

XX век стал веком автоматизации в самых разных областях человеческой деятельности (наука, промышленность, финансы, быт). Примером внедрения автоматизации могут служить разнообразные системы управления, созданные для обеспечения надежного контроля и управления функционированием как отдельных технических устройств, так и целых предприятий.

Широкомасштабное внедрение средств автоматизации стало возможным благодаря появлению компьютеров. Бурное развитие вычислительной техники, вылившееся в появление компьютеров различной производительности и назначения, в свою очередь стимулировало развитие систем передачи цифровой информации. Кульминацией развития сетей стал Интернет.

С ростом популярности Интернета и появлением новых технологий в жизнь многих фирм, а также частных лиц, входит электронная коммерция. Теперь у каждого пользователя персонального компьютера появилась возможность за относительно небольшие деньги получить доступ к практически любому информационному ресурсу.

Сейчас электронные коммуникации стали частью глобальной экономики. Люди используют компьютеры для хранения и передачи все большего количества данных. Вполне естественно, что в этом электронном мире растет потребность в защите информации. Сетевые программы (например, для работы с электронной почтой и электронными денежными переводами) нуждаются в безопасных средствах шифрования и аутентификации. Эти средства должны быть свободно доступны и не ограничены какими-либо государственными, корпоративными или международными препонами.

Криптография обеспечивает конфиденциальность персональных данных, таких как медицинские карты, финансовая информация и электронная почта. В современном обществе, буквально пронизанном сетями, возрастает вероятность того, что эти данные будут украдены или использованы ненадлежащим образом.

Американский программист Зиммерман написал пакет программ для обмена сообщениями по электронной почте, получивших название PGP (Pretty Good Privacy). Пакет удачно совместил в себе возможность шифрования сообщений симметричными блочными алгоритмами, распределения симметричных ключей с помощью асиммет-

ричного алгоритма шифрования RCA, а также создания электронных подписей сообщений. Предполагая возможное вмешательство правительства США в будущем, Зиммерман вместе с программой распространял и исходные тексты программы, положив начало традиции, поддерживаемой до настоящего времени.

Развитие электронной торговли, признания права людей на защиту неприкосновенности их частной жизни, стремление повысить безопасность в Интернете — все это стало причиной широкого распространения криптографии.

Пособие рассчитано на обучение в течение восьми дней.

1-й день — изучение основных понятий информационной безопасности.

2-й день — введение в мир криптографии.

3-й день — знакомство с возможностями системы PGP.

4-й день — посвящен установке PGP на персональный компьютер.

5-й день — изучение приемов шифрования с помощью PGP.

6-й день — изучение приемов создания цифровой подписи.

7-й день — посвящен различным манипуляциям с ключами в среде PGP.

8-й день — изучение приемов шифрования жестких дисков в среде PGP.

1-й день. Информационная безопасность

Петушок с высокой спицы
Стал стеречь его границы.
Чуть опасность где видна,
Верный сторож как со сна
Шевельнется, встрепенется,
К той сторонке обернется
И кричит: «Кири-ку-ку.
Царствуй, лежа на боку!»
И соседи присмирели,
Воевать уже не смели:
Такой им царь Дадон
Дал отпор со всех сторон!

А.С. Пушкин. Сказка о золотом петушке

1.1. Электронная коммерция

Рынок современного общества формируется и развивается на фоне глобализации и интенсивной информатизации мировой хозяйственной системы. Таким же образом, как железные дороги способствовали формированию национальных экономик и рынков, глобальные вычислительные сети способствовали образованию глобальных мировой экономики и мирового рынка [9].

Широкое внедрение Интернета не могло не отразиться на развитии электронных форм бизнеса, одной из которых является электронная коммерция.

Многие крупные компании уже давно прибегают к помощи электронной коммерции при проведении деловых операций. Электронный обмен данными (electronic data interchange, EDI) по частным компьютерным сетям начался в 60-х годах. С того же времени банки начали успешно использовать телекоммуникационные сети для электронного перевода денежных средств (electronic funds transfer, EFT). Системы электронной коммерции на базе протоколов EDI (ANSI X.12, EDIFACT) использовались для организации закупок комплектующих, запчастей, сырья у поставщиков. Но эти системы были дороги и поэтому доступны только крупным компаниям [7].

С появлением Интернета ситуация изменилась коренным образом. С ростом популярности Интернета и появлением новых технологий электронная коммерция входит в жизнь многих больших и малых фирм, а также частных лиц. У каждого пользователя персонального

компьютера появилась возможность за относительно небольшие деньги получить доступ к практически любому информационному ресурсу.

Электронная коммерция считается одним из видов электронного бизнеса. В соответствии с документами ООН, бизнес признается электронным, если хотя бы две его составляющие из четырех (производство товара или услуги, маркетинг, доставка товара, расчеты) осуществляются с помощью Интернета [7].

Другое популярное определение электронной коммерции состоит в следующем. Под электронной коммерцией подразумевается продажа товаров, при которой как минимум организация спроса на товары осуществляется через Интернет (обычно для этого используется web-сайт). При этом способ оплаты не имеет значения: расчеты за покупку могут совершаться даже наличными.

Электронная коммерция начиналась с операций купли-продажи и перечисления денежных средств по компьютерным сетям. В ее основе лежала традиционная коммерция. При этом использование электронных сетей добавляло электронной коммерции гибкости в решении задач организации спроса и расчетов, а также в отдельных случаях и доставки товаров.

Сейчас цели электронной коммерции, с точки зрения бизнеса расширились. Они включают не только операции, прямо связанные с куплей-продажей товаров и услуг для непосредственного извлечения прибыли, но и такие операции, как создание спроса на товары и услуги, организация послепродажной поддержки и обслуживания клиентов, повышение эффективности взаимодействия между деловыми партнерами.

Оперируя цифровой информацией в компьютерных сетях, электронная коммерция предлагает бизнесу принципиально новые возможности, например, облегчает сотрудничество деловых групп.

Коммерческая деятельность через электронные сети снимает ряд физических ограничений, естественных для работы обычных предприятий торговли и сервиса. Компьютерные системы в Интернете способны обеспечивать поддержку клиентов 24 часа в сутки и семь дней в неделю. Заказы на продукцию могут приниматься в любое время и из любого места планеты.

Электронная коммерция развивается на наших глазах: новые технологии и приложения появляются уже прямо сейчас. Это в первую очередь новые средства доступа в Интернет, повышающие возможности клиентов. Например, устройства Set-Top-Box, предназначенные для организации интерактивного телевидения, мобильные телефоны стандарта GSM (ожидается, что именно мобильный телефон станет самым распространенным средством проведения покупок), карманные персональные компьютеры (Personal Digital Assistant, PDA) [7].

1.2. Сбои информационных систем

Сегодня информатизация общества приобретает интенсивный глобальный характер. Интенсивная информатизация подразумевает повсеместное использование принципа «клиент-сеть», а основной парадигмой становится человеко-машинное общество [9]. И следствием лавинообразного распространения компьютерных систем и их взаимодействия посредством сетей возникает все большая зависимость как организаций, так и отдельных людей от информации, хранящейся в связанных сетями системах.

Вирусы, электронная разведка, мошеннические транзакции, совершенные с помощью украденных реквизитов пластиковых карт, интернет-магазины бесследно исчезающие с рынка после успешно исполненных афер, — все это постоянные спутники сегодняшней коммерции. Поэтому вопросы безопасности не могут оставаться второстепенными.

Все это заставляет осознать необходимость защиты данных и ресурсов, использования специальных средств проверки аутентичности получаемых данных, а также защиты систем от несанкционированного доступа и сетевых атак [4].

Компьютерная безопасность и безопасность информационных систем — понятия близкие, так как в обоих случаях имеется в виду защита информационных технологий от сбоев.

Автоматизированным информационным системам могут угрожать случайные или умышленные сбои. Выделяют следующие виды сбоев:

- ошибки, природные явления, атаки, фальсификации, злоумышленное кодирование, взлом [6].

Проблемы с информационными системами чаще всего возникают из-за **ошибок.** В их число входят: ошибки в процессе изготовления

или при сборке технического оборудования; при проектировании системы, обычно связанные с упущениями при анализе задачи; при вводе данных; программировании; небрежности со стороны людей, работающих с данной технологией. Ошибки были и будут всегда. Но ошибки ввода данных в настоящее время удалось снизить благодаря использованию штрих-кодов и автоматического распознавания текста. И на первое место вышли ошибки проектирования и программирования.

Природные явления — это неожиданное насильственное нарушение работоспособности информационной системы без вмешательства человека, например, последствия наводнений, гроз.

Атаки — это самый частый вид умышленных угроз со стороны «чужих». Эти угрозы включают материальные повреждения компьютерного оборудования, рабочих комнат. Это и физические атаки на компьютерные установки, такие как злоупотребление, подслушивание, взлом, заимствование прав. Это может быть и просмотр мусора в поисках паролей.

Фальсификация — это наиболее распространенная умышленная угроза со стороны «своих». Она включает ввод ложной информации в систему, использование компьютерных технологий для создания неверных данных или замену исходной информации. Информационная система продолжает нормально работать, но цели ее работы изменены. Фальсификация составляет большую часть мошенничества в области компьютерных технологий.

Злоумышленное кодирование — это нелегальные программы и фрагменты программ, выполняемые на системных компьютерах. Эти программы могут изменять данные, делать доступной секретную информацию. Существует большое количество типов злоумышленного кодирования: «логические бомбы», «троянский конь», «вирус», «червяк» и др.

Взлом — это проникновение в компьютерную систему или программу путем разгадывания или расшифровки кодов доступа, номеров счетов, паролей.

Умышленные угрозы имеют мотив — это может быть мошенничество, шпионаж, вандализм.

Мошенничество — это использование информационных ресурсов путем умышленного обмана в целях получения незаконной прибыли.

Поскольку большинство ценных товаров (деньги, сырье) запрашиваются через компьютеры, то простое коммерческое мошенничество все чаще осуществляется путем компьютерных атак.

Шпионаж имеет целью получение информации, не подлежащей огласке. Конечным результатом шпионажа является неизбежное снижение информационной ценности данных.

Вандализм — это преднамеренное или злоумышленное повреждение компьютерных ресурсов, включая оборудование, данных и программного обеспечения. Мотивы вандализма могут быть самые разные: озорство юных программистов-взломщиков, личная месть со стороны уволенных служащих, терроризм, военные атаки.

1.3. Стандартные меры безопасности от сбоев

Программы безопасности информационных систем устанавливают меры безопасности, которые должны быть приняты для защиты информационных систем от сбоев. Безопасность информационных систем часто неправильно понимается лишь как вопрос резервного копирования. Это происходит из-за того, что корректное копирование данных и процедуры восстановления совместно с профилактикой линий связей предохраняют от большей части сбоев. Однако чаще всего сбои происходят из-за ошибок, сделанных людьми. Поэтому меры безопасности могут быть самые разные: сюда входят и люди, которые выполняют определенные процедуры, и техническое обеспечение, осуществляющее шифрование.

К стандартным относят следующие меры безопасности:

- контроль доступа, шифрование, электронные подписи и аутентификация, антивирусные программы, процедуры восстановления, защита от сбоев в электропитании, аудит электронной обработки данных, размещение, надежные конфигурации, аварийная сигнализация, противопожарное оборудование, страхование [6].

Контроль доступа ограничивает физический или логический доступ к системам. Физически доступ может быть ограничен оснащением помещений дверными замками, охраной, изучением прошлого служащих. Логический доступ может быть ограничен при помощи систем паролей, программ управления доступом к базе данных, программ безопасности и надежного аппаратного обеспечения.

При **шифровании** данные обрабатываются специальной шифрующей программой (например, PGP), что не дает злоумышленникам возможности восстановить данные из зашифрованного текста. Для этого требуется ключ, при помощи которого и происходит шифрование и расшифровка текста.

К незашифрованным сообщениям могут быть добавлены блоки **подписи** и **аутентификации** (например, с помощью программы PGP), так что получатели смогут удостовериться в том, что сообщение не было изменено и что послание пришло от предполагаемого отправителя.

Антивирусное программное обеспечение включает программы, сканирующие диски и память в поисках кодов вируса, программы мониторинга, которые отслеживают подозрительную активность, ассоциированную с деятельностью вирусов, программы восстанавливающие инфицированные программы до их исходного состояния.

Процедуры восстановления включают резервное копирование на серверах и рабочих станциях пользователей. Данные хранящиеся на серверах копируются на специальное устройство для резервирования, так что содержимое испорченного диска всегда может быть восстановлено. Резервное копирование — это основная корректирующая мера безопасности, необходимая для восстановления работоспособности при любых серьезных сбоях. Поэтому обычно создается несколько резервных копий, и по крайней мере одна из них хранится в удаленном от сервера месте, например, в сейфе.

Защита от сбоев **в питании** и защита коммуникационных линий включает устранение недопустимых скачков напряжения или повышения напряжения в линиях, которые могут быть подвержены воздействию молний или сбоям электропитания. Источники бесперебойного питания обеспечивают постоянное питание от батарей на короткие периоды отключения напряжения.

Функции **аудита электронной обработки данных** включают проверку процессов обработки информации, стандартную проверку информационных систем и проверку проектов приложений на предмет их соответствия принятым стандартам.

Размещение материальных ресурсов информационных систем должно быть таково, чтобы система была наименее уязвима в случае сбоев. Плохие условия размещения компьютеров — это комнаты на

первых этажах, расположение в районах с ненадежным электроснабжением.

Надежные конфигурации подразумевают проектирование информационных систем с распределенной обработкой и хранением, резервные коммуникационные линии и распределенное управление. Устойчивые информационные системы должны функционировать даже в поврежденном состоянии.

Аварийная сигнализация определит причину сбоя и привлечет внимание в случае пожара, кражи, отключения электроэнергии, повреждения линий связи, выхода из строя компьютерных систем.

Противопожарное оборудование включает разбрызгиватели, огнетушители и другие средства тушения пожаров.

К мерам безопасности относится и **страхование,** которое может покрыть потери, вызванные повреждением информационной системы.

1.4. Три аспекта защиты информации

Для того, чтобы понять истинные потребности компании в средствах защиты и выбрать необходимые средства и систему мер безопасности, следует применять систематический подход. Один из таких подходов состоит в рассмотрении следующих трех аспектов защиты информации [4]:

- **Нарушения защиты** — это любые действия, компрометирующие безопасность хранения и использования принадлежащей организации информации.
- **Механизмы защиты** — это механизмы выявления и предотвращения нарушений защиты, а также ликвидации последствий таких нарушений.
- **Службы защиты** — это сервисные службы, предназначенные для противодействия попыткам нарушить защиту на основе использования одного или нескольких механизмов защиты.

1.5. Службы защиты информации

Функции служб защиты можно сравнить с действиями, обычно выполняемыми по отношению к реальным документам. Многие сферы человеческой деятельности, даже такие разные, как коммерция и личная жизнь, связаны с использованием документов и обеспечением

целостности и достоверности этих документов. Документы обычно скрепляются подписью и помечаются датой, они могут требовать защиты от разглашения, подделки или уничтожения, нотариального или свидетельского заверения, регистрации.

С тех пор как использование информационных систем стало жизненно необходимым для ведения многих дел, электронная информация взяла на себя роль, которая традиционно отводилась бумажным документам. Поэтому операции, которые ранее выполнялись при обработке бумажных документов, теперь должны выполняться в отношении документов, существующих в электронном виде. Однако выполнение этих операций не совсем простое дело. И причина в том, что электронные документы имеют особые свойства.

В подавляющем большинстве случаев оригинальный бумажный документ можно отличить от его копии. Но электронный документ — это последовательность битов, поэтому между оригиналом и любой его копией нет никакого различия вообще.

Изменение бумажного документа оставляет следы физического воздействия на этот документ. Так, использование ластика делает бумагу в месте трения более тонкой по сравнению с остальными участками листа. Изменение битов в памяти компьютера не оставляет никаких физических следов.

Процесс заверения физического документа выражается в физических характеристиках этого документа (например, в индивидуальности почерка подписавшего документ лица или в особенностях оттиска печати). А любое подтверждение аутентичности электронного документа должно базироваться на некотором внутреннем доказательстве, заключенном в самой получаемой информации.

Приведем перечень некоторых традиционно выполняемых с бумажными документами операций:

- идентификация, авторизация, лицензирование и сертификация, подпись, освидетельствование, согласование, обязательство, квитанции, сертификация происхождения, передаточная надпись, ограничение доступа, ратификация, учет времени появления, аутентификация, голосование, указание авторства, регистрация, одобрение/неодобрение, секретность.

Аналогичные действия требуются и при работе с электронными документами и сообщениями. Этот перечень можно рассматривать

как список функций, которые желательно иметь в любой системе, обеспечивающей защиту данных. Но этот перечень слишком большой.

Одним из используемых на практике наборов функций защиты является следующий:

- конфиденциальность, аутентификация, целостность, невозможность обмана, управление доступом [4].

Средства обеспечения **конфиденциальности** призваны защитить поток данных от пассивных атак.

Сервис **аутентификации** предназначен для того, чтобы обеспечить надежную идентификацию источника информации. То есть задачей службы является проверка того, что источником такого сообщения является именно тот объект, за который выдает себя отправитель.

Средства защиты **целостности** имеют дело с потоком сообщений и обеспечивают гарантию того, что принятые сообщения будут в точности соответствовать отправленным, без изъятий, дополнений, изменений в исходном порядке следования и повторов.

Средства, гарантирующие **невозможность обмана,** должны не позволить отправителю или получателю отказаться от факта пересылки сообщения.

Управление доступом означает возможность ограничивать доступ к узлам сети и приложениям по каналам связи.

1.6. Механизмы защиты информации

Не существует единого механизма, который мог бы выполнить все функции защиты. Но в основе большинства механизмов защиты лежат методы криптографии. Шифрование или близкое к шифрованию преобразование информации являются наиболее распространенными методами защиты данных.

1.7. Нарушения защиты информации

Попытки нарушения защиты компьютерной системы можно классифицировать, рассмотрев функции компьютерной системы как объекта, предоставляющего информацию. В общем случае мы имеем дело с потоком информации от некоторого источника (например, из файла) в направлении адресата информации (например, в другой файл). Нормальный поток изображен на рис. 1а [10]. Остальные части

рис. 1 иллюстрируют четыре типа атак (нарушений нормального потока информации): разъединение, перехват, модификация, фальсификация [4].

Разъединение (interruption). При такой атаке (рис. 1b) ресурс системы уничтожается, становится недоступным или непригодным к использованию. При этом нарушается доступность информации. Примерами такого типа нарушений могут служить вывод из строя оборудования (например, жесткого диска), обрыв линии связи.

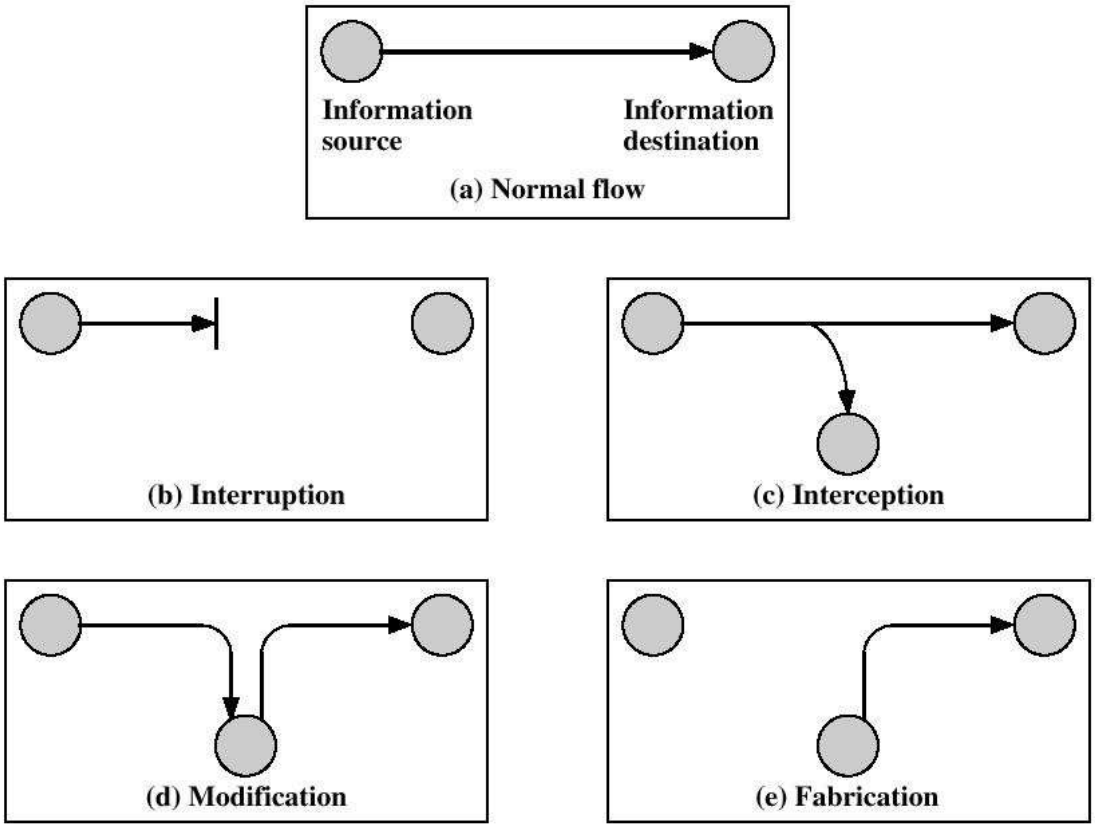

Рис. 1. Угрозы безопасности

Перехват (interception). Здесь к ресурсу открывается несанкционированный доступ (рис. 1c). При этом нарушается конфиденциальность информации. Нарушителем может быть физическое лицо, программа или устройство. Примерами такого типа нарушений являются подключение к кабелю связи с целью перехвата данных и незаконное копирование файлов.

Модификация (modification). В этом случае к ресурсу открывается не только несанкционированный доступ, но и сам ресурс изменяется нарушителем (рис. 1d). При этом нарушается целостность информации. Примерами такого типа нарушений являются изменение зна-

чений в файле данных, модификация программы с целью изменения ее функций.

Фальсификация (fabrication). Здесь в систему вносится подложный объект (рис. 1е). При этом нарушается аутентичность информации. Примером такого нарушения может служить отправка поддельного сообщения по сети.

Другую классификацию нарушений можно представить на основе пассивных и активных атак [4].

Пассивные нарушения защиты (пассивные атаки) носят характер перехвата передаваемых данных. Целью нарушителя является получение передаваемой информации. Пассивные нарушения разделяют на две группы: **раскрытие содержимого сообщений** (release of message contents) и **анализ потока данных** (traffic analysis).

Любое сообщение: телефонный разговор, сообщение электронной почты, пересылаемый файл, может содержат конфиденциальную информацию. И желательно, чтобы с передаваемой информацией не могли ознакомится те, кому эта информация не предназначена.

Другой тип нарушений — анализ потока данных — чаще всего используется тогда, когда для маскировки содержимого применяется шифрование. В этом случае содержимое вполне надежно скрыто. Но у нарушителя остается возможность наблюдать характерные признаки передаваемых сообщений. Например, можно обнаружить и определить отправителя и используемые для отправки сообщения узлы, выяснить частоту обмена сообщениями, их длину. Такая информация может оказаться весьма полезной при определении причины и сути наблюдаемого обмена данными.

Активные нарушения (активные атаки) — это нарушения связанные либо с изменением потока данных, либо с созданием фальшивых потоков. Их разделяют на четыре группы: имитация, воспроизведение, модификация сообщений и помехи в обслуживании [4].

Имитация (masquerade) — означает попытку одного объекта выдать себя за другой.

Воспроизведение (replay) — представляет собой пассивный перехват блока данных в последующую ретрансляцию перехваченный данных с целью получения несанкционированного эффекта.

Модификация сообщений (modification of message contents) — означает либо изменение части легитимного сообщения, либо изменение порядка поступления сообщений с целью получения несанкционированного эффекта.

Помехи в обслуживании (denial of service) — создают препятствия в нормальном функционировании средств связи или управлении ими. Такие нарушения могут иметь вполне конкретную цель, например, объект может задерживать все сообщения, направляемые определенному адресату.

1.8. Модель защиты

Вильям Столлингс [4] предложил модель защиты сети, которая представлена на рис. 2. Кратко описать эту модель можно следующим образом.

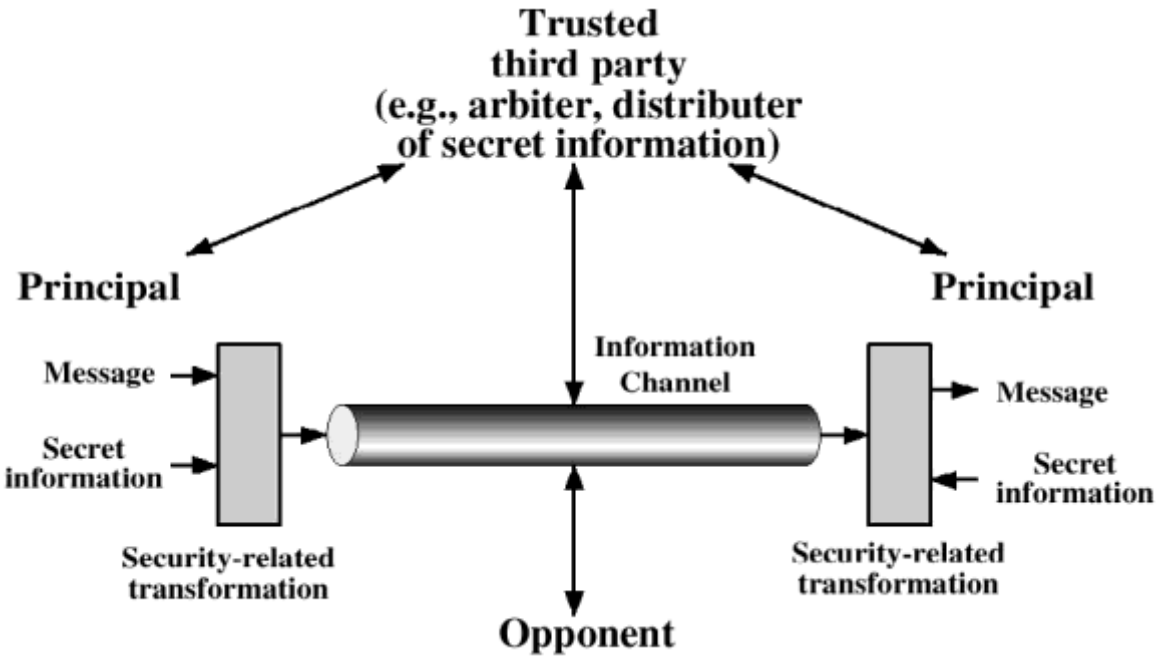

Рис. 2. Модель защиты

Пусть требуется передать **сообщение** (message) одной участвующей в передаче стороны другой через связывающую их сеть. Чтобы обмен информацией состоялся, обе стороны, называемые **доверителями** транзакции (principal), должны вступить во взаимодействие. С этой целью создается логический **информационный канал** (information channel), для чего определяется маршрут прохождения данных от источника к адресату, выбирается коммуникационный протокол (например, TCP/IP).

Вопросы безопасности возникают тогда, когда необходимо обеспечить защиту передаваемой информации от некоторого потенциального **противника** (opponent), который может угрожать конфиденциальности, аутентичности. При этом любая технология защиты имеет две составляющие:

- Обеспечивающее защиту **преобразование передаваемой информации** (security-related transformation). Примерами таких преобразований являются шифрование сообщения, в результате чего противник лишается возможности это сообщение прочесть, и

добавление зависящего от сообщения кода, по которому адресат сможет идентифицировать отправителя.

- Использование некоторой **секретной информации** (secret information), общей для обеих участвующих в транзакции сторон и которая должна оставаться неизвестной противнику. Примером такой секретной информации может быть ключ шифра.

Для обеспечения защиты может понадобиться участие **третьей стороны** (arbiter), заслуживающей доверия обоих участников транзакции. Так, третья сторона может потребоваться для гарантии аутентичности передаваемого сообщения.

1.9. Горячие слова*

* В разделе использованы материалы из [17].

Авторизация — представление субъекту некоторых прав доступа к информационному обмену.

Анализ рисков — процесс определения угроз, уязвимостей, возможного ущерба, а также контрмер.

Аппаратный ключ — физическое приспособление, используемое для защиты компьютерной системы от несанкционированного доступа.

Аутентификация — проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Безопасность информации — состояние информации, информационных ресурсов, информационных и телекоммуникационных систем, при котором с требуемой вероятностью обеспечивается защита информации.

«**Белая книга**» («White Book», ITSEC) — базовый европейский стандарт, который определяет критерии, требования и процедуры для создания систем повышенной безопасности.

Вирус компьютерный — наименование большого числа разнообразных вредоносных программ, главной отличительной чертой которых является способность к «самораспространению» при определенных условиях; количество известных вирусов составляет более 15 тысяч.

Владелец документированной информации, информационных ресурсов, информационных продуктов, средств международного информационного обмена — субъект, реализующий полномочия владения, пользования и распоряжения указанными объектами в объеме, устанавливаемом собственником.

Владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, реализующий полномочия владения, пользования и распоряжения указанными объектами в объеме, устанавливаемом законом.

Вычислительная сеть — группа компьютеров и связанных с ними устройств, соединенных средствами связи.

ГОСТ 28147-89 — «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

ГОСТ Р50922-96 — «Защита информации. Основные термины и определения».

ГОСТ Р50739-95 — «Средства вычислительной техники. Защита от несанкционированного доступа к информации».

Гостехкомиссия России (Государственная техническая комиссия при президенте Российской Федерации) — коллегиальный орган государственного управления; одной из главных задач является разработка нормативной, правовой и нормативно-методической базы в области защиты информации и противодействия техническим разведкам.

Документированная информация (документ) — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Доступ к информации — ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

Доступность — возможность за приемлемое время получить от информационной системы требуемую информационную услугу; один из трех основных аспектов информационной безопасности (доступность, целостность, конфиденциальность).

Журнал — файл регистрации или список транзакций, происходящих в компьютере или в сети.

Задание по безопасности — полная комбинация требований, являющихся необходимыми для создания и оценки информационной безопасности конкретной системы или продукта информационных технологий.

Защита вычислительной системы — предохранение вычислительной системы и ее данных от повреждения или потери.

Защита данных — процесс обеспечения сохранности, целостности и надежности обработки и хранения данных.

Защита информации — организационные, правовые, техниче-

ские и технологические меры по предотвращению угроз информационной безопасности и устранению их последствий.

Защита информации от непреднамеренного воздействия — деятельность, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств ИС, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации (ГОСТ 50922).

Защита информации от несанкционированного воздействия — деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав или правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации (ГОСТ 50922).

Защита информации от несанкционированного доступа — деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или владельцем информации прав или правил доступа к защищаемой информации (ГОСТ 50922).

Защита информации от разглашения — деятельность, направленная на предотвращение несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации (ГОСТ 50922).

Защита информации от технической разведки — деятельность, направленная на предотвращение получения защищаемой информации разведкой с помощью технических средств (ГОСТ 50922).

Защита от несанкционированного доступа — предотвращение или существенное затруднение несанкционированного доступа.

Защищённое средство вычислительной техники — средство вычислительной техники, в котором реализован комплекс средств защиты.

Защищённые системы — системы, в которых обеспечивается защита информации с использованием шифровальных средств, защищённого оборудования и организационных мер.

Злоумышленник — пользователь или программа, неправомочно (несанкционированно) пытающиеся получить доступ к отдельному

компьютеру или сети.

Идентификатор — уникальный признак субъекта или объекта доступа.

Идентификация — присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

ИКСИ — Институт криптографии, связи и информатики (http://www.fssr.ru).

Интернет-протоколы — совокупность соглашений, зафиксированных в стандартах и реализующих их программных средств, которые обеспечивают выполнение базовых элементарных процедур функционирования Интернета; основными защищенными протоколами являются: https, smtps, nntps, ftps, telnets, imaps, ircs, pop3s.

Информационная безопасность — защищенность ресурсов ИС от факторов, представляющих угрозу для конфиденциальности, целостности, доступности.

Информационная инфраструктура — совокупность центров обработки и анализа информации, каналов информационного обмена и телекоммуникации, линий связи, систем и средств защиты информации.

Информационная революция — термин, используемый в отношении текущего периода человеческой истории, характеризующийся тем, что владение и распространение информации вытеснило механизацию или индустриализацию как движущую силу в обществе.

Информационная система — комплекс, включающий вычислительное и коммуникационное оборудование, программное обеспечение, лингвистические средства и информационные ресурсы, системный персонал, обеспечивающий поддержку динамической информационной модели некоторой части реального мира для удовлетворения информационных потребностей пользователей [18].

Информационные процессы — процессы создания, сбора, обработки, накопления, хранения, поиска, распространения и потребления информации.

Информационные ресурсы — отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

Информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Категорирование защищаемой информации — установление градации важности защищаемой информации (ГОСТ 50922).

Комплекс средств защиты — совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации.

Конфиденциальная информация — документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Криптографическая защита — защита данных при помощи криптографического преобразования данных (ГОСТ 28147).

Лицензирование в области защиты информации — деятельность, заключающая в передаче или получении прав на проведение работ в области защиты информации и осуществлении контроля за лицензиатом.

Объект информационного обмена — пассивная единица информационного обмена, например, файл, каталог, электронное письмо, пароль, электронная подпись и др.

Объект защиты информации — информация, носитель информации, информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации (ГОСТ 50922).

«**Оранжевая книга»** («Orange Book», TCSEC) — стандарт Министерства обороны США, содержащий требования к средствам обеспечения безопасности компьютерных систем, который имеет основополагающее значение не только для США, но и для всей международной системы стандартов в области информационной безопасности). Отечественный аналог — Руководящий документ Гостехкомиссии РФ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации. 1992».

Пользователь (потребитель) информации — субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Программа для ЭВМ — это объективная форма представления совокупности данных и команд, предназначенных для функционирования электронных вычислительных машин (ЭВМ) и других компьютерных устройств с целью получения определенного результата.

Программное средство — программа, предназначенная для

многократного применения на различных объектах разработчика любым способом и снабженная комплектом программных документов (ГОСТ 28195-89).

Программное обеспечение АС — совокупность программ на носителях данных и программных документов, предназначенных для отладки, функционирования и проверки работоспособности АС (ГОСТ 34.003-90).

Программный продукт — набор компьютерных программ, процедур и связанная с ними документация и данные (ISO/IEC 12207-95).

Ресурс — в широком смысле это все, что представляет ценность с точки зрения организации и является объектом защиты; классы ресурсов: оборудование, информационные ресурсы, программное обеспечение, сервис и поддерживающая инфраструктура.

Сертификация средств защиты информации — надлежащим образом оформленный документ, выданный по правилам системы сертификации и подтверждающий соответствие средства защиты информации требованиям по безопасности информации, предъявляемым ФАПСИ.

Система защиты информации — совокупность органов и исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации (ГОСТ 50922).

СОРМ — система технических средств по обеспечению оперативно-розыскных мероприятий; разработана ФСБ и внедряется на основании Закона РФ от 12.08.95 № 144-ФЗ.

Средства защиты информации — технические, криптографические, программные и другие средства, предназначенные для защиты информации, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Субъект информационного обмена — активная единица информационного обмена, некоторое приложение или процесс операционной системы.

Требования по безопасности информации — руководящие документы ФАПСИ, регламентирующие качественные и количественные критерии безопасности информации и нормы эффективности ее защиты.

Уровень сертификата ФАПСИ — в зависимости от полноты ре-

ализуемой защиты, для системы конфиденциального документооборота устанавливаются три уровня обеспечения безопасности: уровень A, B, C.

ФАПСИ (Федеральное агентство правительственной связи и информации при президенте Российской Федерации) — является органом, осуществляющим обязательное лицензирование деятельности юридических и физических лиц, связанную с разработкой, производством, реализацией и эксплуатацией шифровальных средств, а также защищенных технических средств хранения, обработки и передачи информации, предоставлении услуг в области шифрования информации.

Целостность информации — актуальность и непротиворечивость информации, ее защищённость от разрушения и несанкционированного изменения.

ISO (International Standards Organization) — международная организация стандартов; jтвечает за стандартизацию в разных областях.

ISO 7498-2: 1989 — «Взаимосвязь открытых систем. Базовая эталонная модель. Ч.2: Архитектура защиты информации». Международный стандарт. Определяет 14 факультативных услуг по защите сохранности информации в процессе взаимодействия открытых систем и 8 механизмов, с помощью которых эти услуги выполняются.

2-й день. Начальная криптография

> Наташа не возразила ни слова. Мысль, что тайна ее сердца известна отцу ее, сильно подействовала на ее воображение. Одна надежда ей оставалась: умереть прежде совершения ненавистного брака. Эта мысль ее утешила. Слабой и печальной душой покорилась она своему жребию.
>
> *А.С. Пушкин. Арап Петра Великого*

2.1. Классификация

В основе большинства механизмов защиты информации лежат методы криптографии. **Криптография** — это наука о том, как обеспечить секретность сообщения. А **криптоанализ** — наука о том, как вскрыть шифрованное сообщение, то есть как извлечь открытый текст не зная ключа. Криптографией занимаются криптографы, а криптоанализом занимаются криптоаналитики [12].

Криптография покрывает все практические аспекты секретного обмена сообщениями, включая аутенфикацию, цифровые подписи, электронные деньги и многое другое.

Цель криптографической системы заключается в том, чтобы **зашифровать** (encryption) осмысленный исходный текст (также называемый открытым текстом, plaintext), получив в результате совершенно бессмысленный на взгляд шифрованный текст или **шифротекст** (называемый также криптограммой, ciphertext). Получатель, которому он предназначен, должен быть способен **расшифровать** (decryption) этот шифротекст, восстановив, таким образом, соответствующий ему открытый текст. При этом противник (называемый также криптоаналитиком) должен быть неспособен раскрыть исходный текст. Метод шифровки/расшифровки называют **шифром** (cipher).

Существует важное отличие между расшифровкой и раскрытием шифротекста. Раскрытием криптосистемы называется результат работы криптоаналитика, приводящий к возможности эффективного раскрытия любого, зашифрованного с помощью данной криптосистемы, открытого текста. Степень неспособности криптосистемы к раскрытию называется ее стойкостью.

Существуют несколько способов, в соответствии с которыми могут классифицироваться криптографические системы.

Системы подразделяются на криптосистемы **ограниченного** и **общего** использования [11]. В первом случае — используются алгоритмы шифрования основанные на том, что сам метод шифрования (алгоритм) является секретным. Сейчас такие методы представляют лишь исторический интерес и не имеют практического значения. Во втором случае — алгоритмы используют ключ для управления шифровкой и расшифровкой, то есть сообщение может быть успешно расшифровано только если известен ключ. Все современные алгоритмы относятся именно к этому классу.

Системы общего назначения классифицируются по числу применяемых ключей. Если отправитель и получатель используют один и тот же ключ, то система называется симметричной (системой с одним ключом или системой с **секретным** ключом). Если отправитель и получатель используют разные ключи, то система называется асимметричной (системой с двумя ключами или схемой шифрования с **открытым** ключом).

Другая классификация строится на типе операций по преобразованию открытого текста в шифрованный. Все алгоритмы шифрования основываются на использовании двух операций: **замены,** означающей замещение каждого элемента открытого текста (бита, буквы) некоторым другим элементом, и **перестановки,** означающей изменение порядка следования элементов открытого текста. При этом главным требованием оказывается отсутствие потерь информации, то есть обратимость всех операций. В большинстве реальных схем шифрования применяют не одну, а комбинацию нескольких операций замены и перестановки.

Еще один способ классификации — по методу обработки открытого текста. **Блочное** шифрование предполагает обработку открытого текста блоками, в результате которой получаются блоки шифрованного текста. **Поточное** шифрование подразумевает шифрование элементов открытого текста последовательно, после чего на каждом этапе получается по одному элементу шифрованного текста.

2.2. Криптосистемы ограниченного использования

Криптографическая система является криптосистемой **ограниченного** использования, если ее стойкость основывается на сохранении в секрете самого характера алгоритмов шифрования и расшифровки.

Простейшим историческим примером такой системы можно считать так называемый шифр Цезаря.

Гай Юлий Цезарь не доверял гонцам и использовал в своей переписке шифр собственного изобретения. Применительно к русскому языку он состоял в следующем. Выписывался алфавит: А, Б, В, Г, Д, Е и т.д, затем под ним выписывался тот же алфавит, но со сдвигом на 3 буквы влево:

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Ъ	Э	Ю	Я
Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Ъ	Э	Ю	Я	А	Б	В

Поэтому когда Цезарь отправлял письма своим генералам, то каждую букву А заменял буквой Г, Б заменял на Д, В — Е и так далее. Так, например, слово РИМ превращалось в слово УЛП. Получатель сообщения УЛП искал эти буквы в нижней строке и по буквам над ними восстанавливал исходное слово РИМ. Ключом в шифре Цезаря является величина сдвига нижней строки алфавита. Только тот, кто знал правило «сдвиг на 3» мог расшифровать его послание.

Подобные системы не используются для конфиденциальной связи в современной ситуации, когда должна обеспечиваться работа огромного числа абонентов.

2.3. Криптосистемы с секретным ключом

Криптографическую систему назовем криптосистемой **общего использования**, если ее стойкость основывается не на секретности алгоритмов шифрования и расшифровки, а на секретности некоторого сравнительно короткого значения, которое называется ее **ключом** (key) [11].

Такой ключ должен легко вырабатываться конкретными пользователями при помощи их собственных ключей таким образом, чтобы даже разработчик криптосистемы не мог раскрыть ее, не имея доступа к тому ключу, который в ней в действительности использовался.

Для некоторых применений (главным образом в военных, дипломатических и разведывательных ведомствах) для разработчика общей криптосистемы нет никаких причин для того, чтобы открытым образом описывать характер ее алгоритмов. Сохраняя эту информацию в тайне, можно обеспечить некоторую дополнительную безопасность. Однако, решающим обстоятельством, позволяющим полагаться на та-

кую секретность, это не является, поскольку ничего нельзя сказать о том, когда она может быть скомпрометирована. По этой причине, исследования надежности таких систем всегда должны проводиться в предположении, что потенциальному противнику о криптосистеме известно все, за исключением реально используемого секретного ключа. А если на самом деле противник такими знаниями не обладает, то это даже лучше. Для других типов применений, например, большим финансовым комплексам, в действительности лучше раскрывать, как работают их криптосистемы. В противном случае пользователи всегда будут предполагать возможность существования некоего секретного метода раскрытия такой криптосистемы.

Общая криптографическая система называется **криптосистемой с секретным ключом,** если в ней любые две стороны, перед тем, как связаться друг с другом, должны заранее договориться между собой об использовании в дальнейшем некоторой секретной части информации, которая и называется секретным ключом [11].

Отсутствие необходимости хранить в секрете алгоритм дает производителям возможность реализовать алгоритмы шифрования данных в виде дешевых общедоступных микросхем, которыми оснащены многие современные системы.

При использовании таких систем основная проблема защиты заключается в надежном сохранении секретного ключа.

Наиболее важными алгоритмами традиционной схемы шифрования (или систем с секретным ключом) являются блочные шифры DES, IDEA.

Предположим, Серёга желает отправить сообщение для Натали, и хочет, чтобы никто, кроме нее, не смог его прочитать. Как показано на рис. 3, можно зашифровать, то есть преобразовать сообщение безнадежно сложным образом, зная, что никто, кроме Серёги и Натали, не сможет его прочитать. При этом Серёга применяет для шифрования криптографический ключ, а Натали должна использовать тот же ключ для расшифровки.

Здесь один и тот же ключ используется как для зашифровки, так и для расшифровки сообщения. Это означает, что этот ключ должен быть сначала передан по надежному каналу, с тем чтобы обе стороны знали его до того, как передавать зашифрованное сообщение по ненадежному каналу.

Но возникает вопрос: если у Серёги есть надежный канал, которым он может воспользоваться для обмена ключами, спрашивается, зачем ему вообще нужна криптография?

2.4. Схема шифрования с секретным ключом

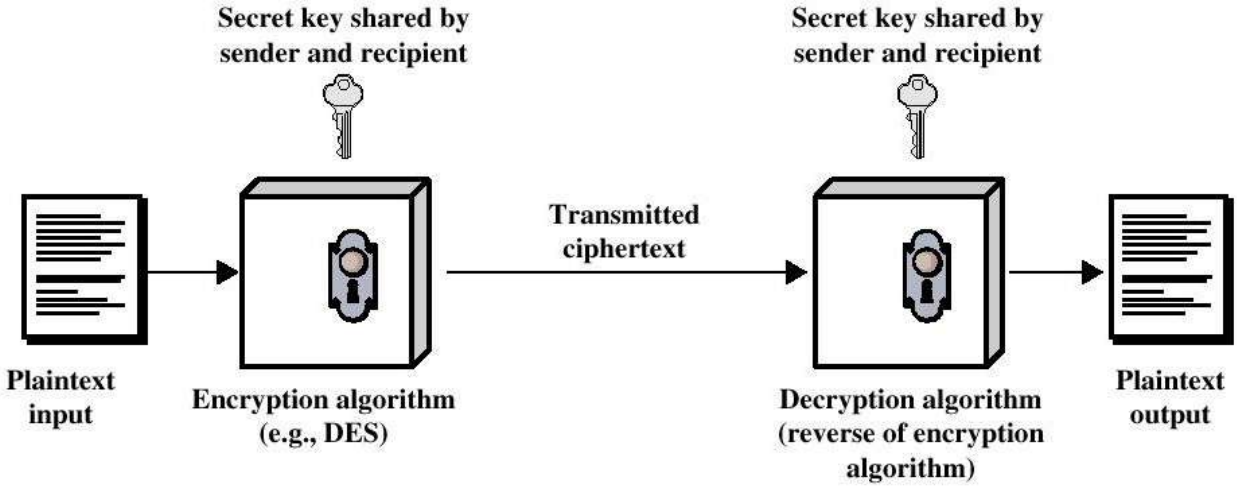

Рис. 3. Упрощенная модель шифрования с секретным ключом

Схема шифрования с секретным ключом (рис. 3) складывается из следующих пяти составляющих:

- **Открытый текст** (plaintext). Это исходное сообщение или данные (plaintext input), подаваемые на вход алгоритма шифрования.
- **Алгоритм шифрования** (encryption algorithm). Алгоритм, выполняющий различные подстановки и преобразования в открытом тексте.
- **Секретный ключ** (secret key). Секретный ключ также подается на вход алгоритму. От этого ключа зависят конкретные подстановки и преобразования, выполняемые алгоритмом.
- **Шифрованный текст** (ciphertext). Это “перемешанное” сообщение, получаемое на выходе алгоритма. Оно зависит от открытого текста и секретного ключа. Для одного и то же сообщения два разных ключа порождают разные шифрованные тексты.
- **Алгоритм расшифровки** (decryption algorithm). Это алгоритм шифрования, выполняемый в обратную сторону. Он берет шифро-

ванный текст и тот же секретный ключ, который применялся при шифровании, и восстанавливает исходный открытый текст.

2.5. Криптосистемы с открытым ключом

Вспомните персонаж из шпионского фильма: человек с запечатанным дипломатом, пристёгнутым наручником к запястью. Что в этом дипломате? Там не коды запуска ракет. Там — ключ, который расшифрует секретную информацию.

Для установления зашифрованных коммуникаций, использующих систему с секретным ключом, отправителю и получателю нужно прежде согласовать ключ и держать его в тайне. Если они находятся в физически удалённых местах, то должны прибегнуть к помощи доверенного посредника, как, например, курьера, чтобы избежать раскрытия ключа в процессе передачи. Каждый, перехвативший ключ в пути, сможет позднее читать, изменять и подделывать любую информацию, зашифрованную или заверенную данным ключом.

Потребность в секретном распределении ключей не была непреодолимой проблемой в те дни, когда криптография использовалась небольшим числом пользователей. Теперь же, когда криптография стала общедоступной, было бы неразумно организовывать такую сеть, в которой каждой паре потенциальных пользователей заранее предоставлялся бы их совместный секретный ключ, потому что тогда число таких ключей возрастало бы квадратично с увеличением числа пользователей.

В 1976 году Диффи и Хеллман заложили основы для преодоления этой трудности, предложив понятие **криптографии с открытым ключом.** Вскоре последовала его первая практическая реализация, предложенная Райвестом, Шамиром и Адлманом.

Секретная связь по незащищенным каналам связи между двумя совершенно незнакомыми друг с другом сторонами наконец-то стала возможна.

Основное наблюдение, которое, собственно, и привело к криптографии с открытым ключом, заключалось в следующем — тот, кто зашифровывает сообщение, необязательно должен быть способен его расшифровывать. В таких системах каждый пользователь выбирает свой собственный секретный ключ, на основании которого получает пару алгоритмов. Затем он делает один из них доступным каждому из возможных корреспондентов, объявляя этот алгоритм своим открытым алгоритмом шифрования, в то время как другой, соответствующий первому и являющийся его личным алгоритмом расшифровки,

хранит в строгом секрете. Это позволяет даже совершенно незнакомому, например, с абонентом сети по имени Натали, пользователю применять ее общедоступный алгоритм шифрования, чтобы зашифровать предназначенное для нее сообщение. Однако лишь сама Натали сможет расшифровать его после получения с помощью своего секретного алгоритма расшифровки.

Само собой разумеется, что такие системы могут быть стойкими, только если по свойствам общедоступного алгоритма шифрования невозможно “вычислить” или подобрать соответствующий ему алгоритм расшифровки.

Наиболее важными алгоритмами криптографических систем с открытым ключом являются: RSA и алгоритм Диффи-Хеллмана.

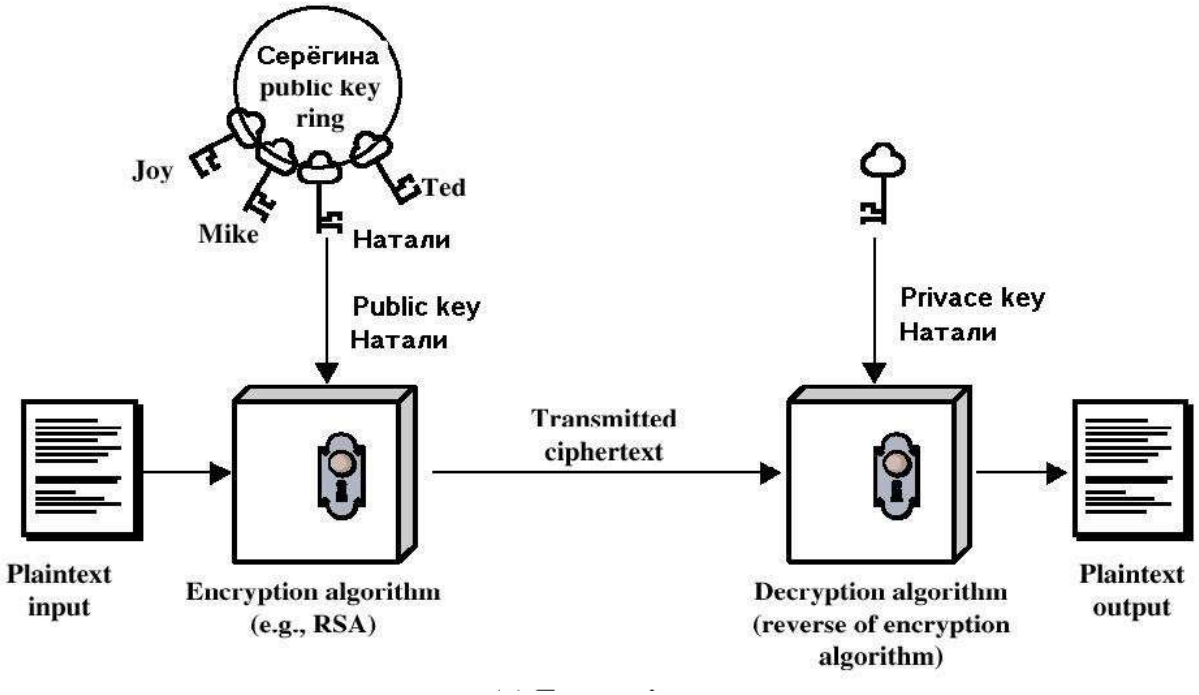

Рис. 4. Криптография с открытым ключом (шифрование)

2.6. Схема шифрования с открытым ключом

Схема шифрования с открытым ключом (рис. 4) складывается из следующих компонентов:

- **Открытый текст** (plaintext). Это исходное сообщение или данные, подаваемые на вход алгоритма шифрования.
- **Алгоритм шифрования** (encryption algorithm). Алгоритм, выполняющий определенное преобразование открытого текста.

- **Открытый** (public key) и **личный** (privace key) ключи. Пара ключей, выбираемых таким образом, чтобы тогда, когда один из них применяется для шифрования, второй можно было бы использовать для расшифровки.
- **Шифрованный текст** (ciphertext). Перемешанный текст сообщения, получаемый на выходе алгоритма. Зависит от открытого текста и ключа. Для одного и того же сообщения два разных ключа порождают разные шифрованные тексты.
- **Алгоритм расшифровки** (decryption algorithm). Алгоритм, с помощью которого с использованием соответствующего ключа обрабатывается шифрованный текст, чтобы в результате получился открытый текст.

При такой схеме шифрования выполняются следующие шаги:

- Каждый пользователь создает пару ключей, которые предполагается использовать для шифрования и расшифровки сообщений.

Каждый из ключей, входящих в пару, открытый и личный, подходит для расшифровки сообщения, зашифрованного с применением другого ключа из той же пары. Зная открытый ключ, личный вычислить невозможно.

- Каждый пользователь публикует один из ключей, размещая этот ключ в открытом для всех реестре или доступном другим файле.

Это и есть открытый ключ. Второй ключ, соответствующий открытому, остается в личном владении и должен сохраняться в секрете.

- Собираясь послать Натали сообщение, Серёга шифрует его, используя открытый ключ Натали.
- Натали, получив сообщение, расшифровывает его с помощью своего личного ключа. Другой получатель не сможет расшифровать сообщение, поскольку личный ключ Натали знает только Натали.

В рамках этого подхода все участники имеют доступ к открытым ключам, а личные ключи создаются на месте каждым участником для себя и поэтому их никогда не приходиться распределять. До тех пор пока системе удается сохранять свой личный ключ в секрете, поступающие сообщения оказываются защищенными. В любой момент си-

стема может изменить свой личный ключ и опубликовать соответствующий ему открытый ключ, заменяющий старый открытый ключ.

Ключи, используемые в схемах традиционного шифрования, называются секретными ключами. Пара ключей, используемых в схемах шифрования с открытым ключом, называются открытым ключом и личным ключом. Личный ключ, должен храниться в секрете, но называется личным, а не секретным во избежание путаницы с ключом, используемым в схеме традиционного шифрования.

2.7. Алгоритм шифрования RSA

Самой первой криптосистемой с открытым ключом из предложенных в открытой литературе (1978 г.), была система Райвеста, Шамира и Эдлмана. Она стала известна под названием RSA. Схема RSA получила самое широкое признание и реализована практически во всех приложениях шифрования с открытым ключом. RSA представляет собой блочный шифр, в котором открытый и шифрованный текст представляется целыми числами из диапазона от 0 до n-1 для некоторого n.

Рассмотрим как работает этот алгоритм [5].

Выбор p, q. Чтобы зашифровать и расшифровать что-то, необходима пара ключей — открытый и личный. Для того чтобы их изготовить, понадобится пара простых чисел p и q. Простыми называются числа, которые делятся без остатка только на себя и на единицу. Число 11 — простое, а 4 — нет, так как делится кроме единицы и четверки еще и на 2. Итак, выбираем пару простых чисел p=3, q=7.

Вычисление n. Следующий этап в изготовлении ключей — получение числа n, равного произведению p и q: n=p*q=3*7=21. Это число называют модулем сравнения при шифровании и расшифровке.

Вычисление ϕ (n). Теперь нужно вычислить величину ϕ (n), называемую функцией Эйлера по формуле: (p-1)*(q-1)=2*6=12. Это число не простое, и его в нашем случае можно разложить на простые множители ϕ(n)=12=2*2*3.

Выбор e. Следующий шаг — подбор числа e, которое должно соответствовать двум критериям: быть меньше n и не иметь общих множителей с ϕ (n), то есть в разложении на простые множители числа e не должно быть ни двойки, ни тройки. Этим требованиям удовлетворяет число 5 — оно меньше n, и к тому же простое, то есть ни на какие сомножители не разлагается. Итак, e=5.

Вычисление d. И последнее, надо найти число d такое, что e*d-1 делится ϕ (n). Тогда получается, что d=17, то есть e*d-1=5*17-1=84, а 84/12=7 — то есть действительно делится.

Открытый и личный ключ. Теперь у нас есть и открытый ключ, пара чисел (n,e) — (21,5), и пара чисел (n,d) — (21,17) — личный ключ.

Открытый текст. Далее предположим, что эта пара принадлежит Серёге. Натали, обладая серёгиным открытым ключом, может послать ему в зашифрованном виде количество стуков в дверь — число 3.

Шифрование. Пусть m=3. Чтобы зашифровать это число, Натали должна проделать вычисления согласно формуле:

$c=m^e \bmod n$, где m — шифруемое сообщение, (n,e) — открытый ключ Серёги, c — зашифрованное сообщение.

В нашем случае $m^e = 3^5 = 243$. Тогда c=243 mod 21. Это есть остаток от деления 243 на 21 и равный 12. Итак, зашифрованное число стуков в дверь равно 12. Вот его посылаем Серёге.

Расшифровка. Для расшифровки сообщения Серёга использует формулу:

$m=c^d \bmod n$, где c — зашифрованное сообщение, m — расшифрованное сообщение, (n,d) — личный ключ Серёги (21,17).

Чтобы расшифровать сообщение, придется возвести c в 17-ю степень $12^{17} = 2218611106740436992$.

Колоссальное число, но остаток от деления 2218611106740436992 на 21 равно 3 — Серега расшифровал сообщение от Натали.

Открытый текст. Теперь идя к ней в гости, он знает сколько раз ему стучать в дверь – три раза.

2.8. Цифровая подпись

Предположим, что Серёга хотел бы послать Натали сообщение, содержимое которого он не считает секретным, но желает, чтобы Натали была уверена в том, что сообщение пришло именно от него. В этом случае Серёга использует свой личный ключ для шифрования сообщения.

Когда Натали получит шифрованный текст, она выяснит, что его можно расшифровать только с помощью открытого ключа Серёги. А это докажет, что сообщение могло быть зашифровано только Серёгой. Никто другой не имеет личного ключа Серёги, поэтому никто другой не мог создать шифрованный текст, дешифрируемый открытым ключом Серёги. В этом случае все шифрованное сообщение выступает в роли цифровой подписи.

Но эта схема требует от системы достаточно много ресурсов. Поэтому более эффективным подходом оказывается шифрование небольшого блока данных, являющегося функцией документа.

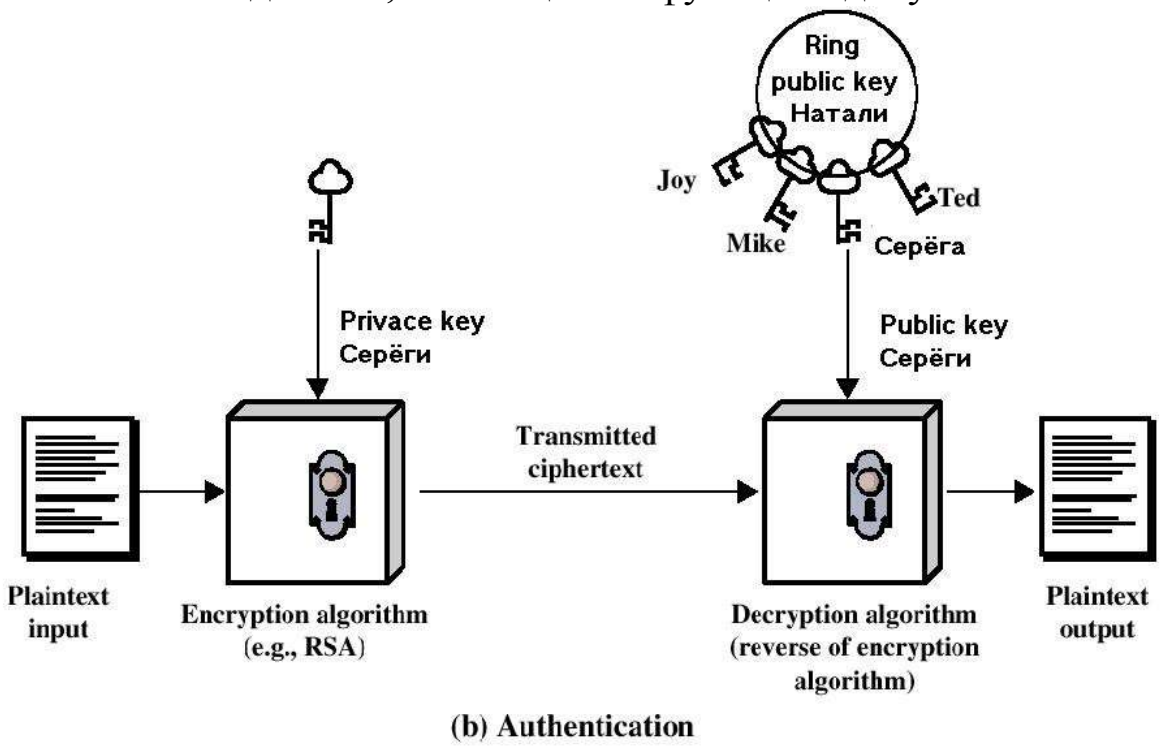

Рис. 5. Криптография с открытым ключом (аутентификация)

В этом случае цифровая подпись документа обычно создается так: из документа генерируется так называемый **дайджест** (message digest) и к нему добавляется информация о том, кто подписывает документ, штамп времени и прочее. Получившаяся строка далее зашифровывается личным ключом подписывающего с использованием того или иного алгоритма. Получившийся зашифрованный набор бит и представляет собой подпись. К подписи обычно прикладывается открытый ключ подписывающего.

Получатель сначала решает для себя доверяет ли он тому, что открытый ключ принадлежит именно тому, кому должен принадлежат и затем расшифровывает подпись с помощью открытого ключа.

Если подпись нормально расшифровалась, и ее содержимое соответствует документу, то сообщение считается подтвержденным (рис. 5).

Важно помнить, что в случае подписи, процесс шифрования не обеспечивает конфиденциальности. То есть пересылаемому таким образом сообщению гарантирована защита от изменения, но не от перехвата.

2.9. Алгоритм цифровой подписи

Пусть Серёга хочет послать Натали то же число 3, но на это раз не зашифрованное, а подписанное цифровой подписью. Чтобы создать подпись он использует свой личный ключ (21,17):

$s=m^d \bmod n$, где s — подпись, m — сообщение.

В нашем случае получается $m^d = 3^{17} = 129140163$. Тогда $s=129140163 \bmod 21$. Остаток равен 12. Итак, Серёга отправляет само незашифрованное сообщение — 3, и подпись равную 12.

Получив сообщение Натали проверяет подпись. Для этого с помощью открытого ключа Серёги ей необходимо проверить, что

$m=s^e \bmod n$, где s — подпись, m — сообщение.

В нашем случае, $m= 12^5 \bmod 21 = 248832 \bmod 21 = 3$.

Все правильно. Сообщение послано действительно Серёгой.

3-й день. Криптографическая система PGP

3.1. Достаточно надежная секретность

Мы в фортеции живем,
Хлеб едим и воду пьем;
А как лютые враги
Придут к нам на пироги,
Зададим гостям пирушку:
Зарядим картечью пушку.

А.С. Пушкин. Капитанская дочка

Рис. 6. Фил Зиммерман

PGP (Pretty Good Privace) — это криптографическая программа, которая обеспечивает конфиденциальность и сервис аутентификации, которые можно использовать для электронной почты и приложений хранения файлов.

В значительной степени PGP является плодом усилий одного человека — Фила Зиммермана (Phil Zimmermann) [19]. По существу, Зиммерман сделал следующее [4]:

- Выбрал в качестве строительных блоков лучшие из доступных криптографических алгоритмов.
- Интегрировал эти алгоритмы в одном приложении, независимом от процессора и операционной системы и построенном на использовании небольшого числа простых команд.
- Объявил пакет, включающий документацию и исходный текст программы, свободно доступным через Интернет.
- Заключил соглашение с компанией Network Associates о разработке и поддержке недорогой коммерческой версии PGP, полностью совместимой с бесплатной.

Система PGP быстро получила признание и стала весьма популярной. Среди причин популярности PGP можно назвать следующие:

- Она широко доступна в бесплатных freeware-версиях, выполняемых на множестве платформ: Windows (95,NT,2000,XP), Unix, MacOS и др. Кроме того, существует коммерческая версия, предназначенная для пользователей, предпочитающих иметь поддержку производителя.

- Система PGP основана на алгоритмах, которые выдержали проверку практикой и считаются исключительно надежными. В частности, в пакет включены алгоритмы шифрования с открытым ключом RCA, DSS и алгоритм Диффи-Хеллмана, алгоритмы традиционного шифрования CAST-128, IDEA и TDEA, а также алгоритм хэширования SHA-1.
- Система PGP имеет очень широкую область применения — от корпораций, которые хотят иметь стандартизованную схему шифрования файлов и сообщений, до простых пользователей, которые нуждаются в защите своей электронной переписки.
- Система PGP не была разработана правительственной или другой официальной организацией и поэтому неподконтрольна им.

3.2. PGP для бизнеса

Главное свойство PGP — она позволяет шифровать и подписывать электронные письма. Удивительно, но все письма, которые мы пересылаем через Интернет находятся в открытом виде [13].

Что это значит? Письмо, посланное по электронной почте «проходит» через несколько Интернет-серверов, на которых письмо можно отловить и прочитать. Например, мы приготовили письмо (рис. 7).

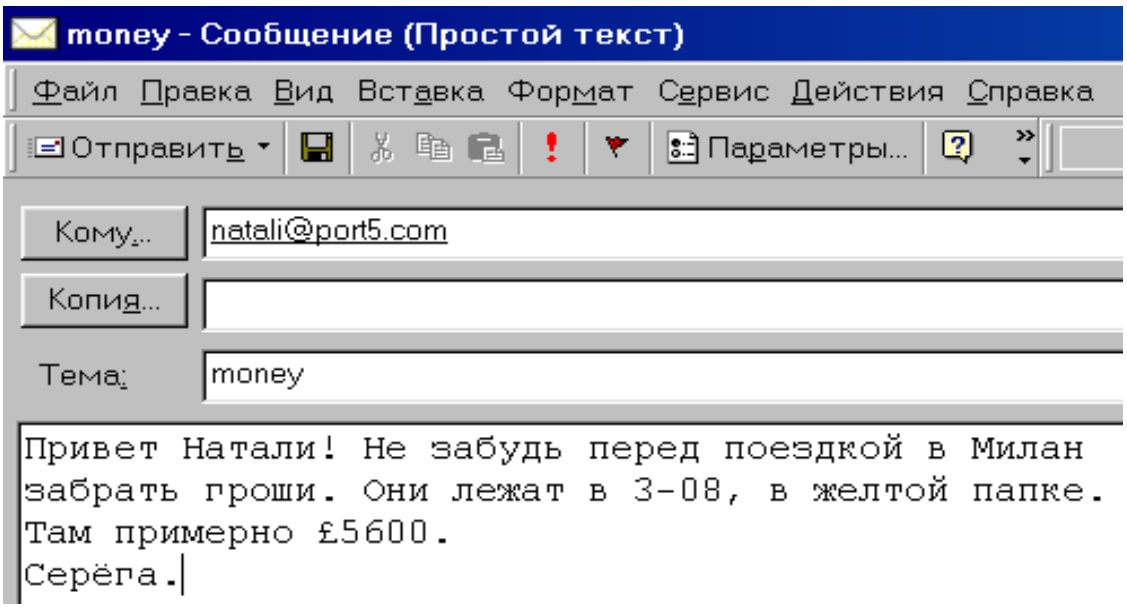

Рис. 7. Сообщение в почтовой программе

Это же письмо можно прочитать и с сервера провайдера (рис. 8)!

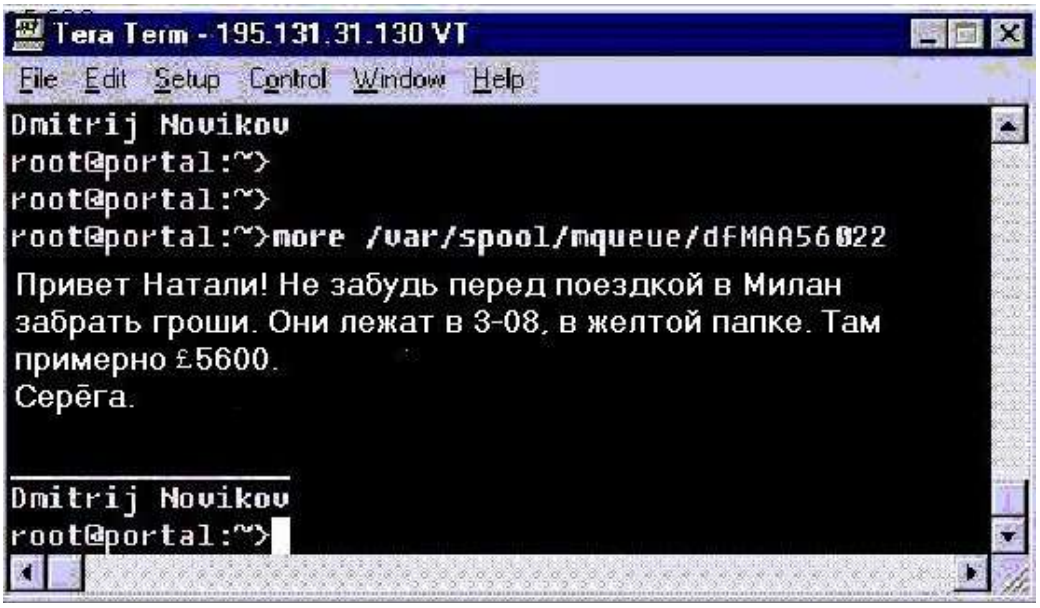

Рис. 8. Сообщение на сервере

Но можно воспользоваться PGP и зашифровать сообщение. А делается это очень просто — нажатием двух кнопочек в Outlook и при отправке письма введением пароля. Теперь сообщение уйдет в шифрованном виде, и взломщик на сервере увидит примерно следующее (рис. 9).

```
root@portal:/etc/namedb>more /var/spool/mqueue/dfSAA35624
-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 6.5.2 for non-commercial use <http://www.pgp.

qANQR1DBwU4DPWAusduWMRYQB/9iNpXcbh22SpYFxQe4ooTn/oY8JPtMpdYZEJWa
q5u7Rj/QU9nb5R8jTO1uGKsnoNLqwnA3H1mB3aGpYfeHXX+DS6rHGLVI5y1BjbMZ
OCFfyvcwJdFsDsvmTolXCnxxW6bY4IcHUaZmLsE/+xPBcpaAk2ZGb/8pytnrKA99
Zmu1hmrSotfwJHMJ/aaQ3eFTyd0HUmiH2plDcImtjUk1UWPoGREba/lcko/775Me
TEKEkKTTrHHROE2agOh+So5iEerPaoAuqZDg8CF2KE/IyVH5rgw8VhP9CEmKejd7
JYxTtYiMcQpshayCgsnQczLdvKoW+TeWkgdv4xt1cLVAEJ6hCACehohhhDMWYe/u
zVnDJN2k2v6DPZtNiPHDo62Id61EW+PjCDA6pbLcqOj2truQ1f0/tHgv5s21SqjW
6URNR/5VDmn4XLwWT4Hhg0ZPKPVSk9SrrB7Fb8Fx2gV/CRA3FRfkjE4WYWkX3hte
LMxU981IXrbcg1svcKSIrMeVwJqXopzs3s90ljdJOurtaVYUKHwwGc3TbVIKb+dU
VdNrG55cywrVFU1CZWp6IUEcgmbc2mB+PFM3AHQOuQq5FNONNdxXPRMQs0BKozv9
vGk3k0zEe1mTvkNjWTtaQ2gScjp+pkbHkogULpOTDI81TAs/T3u1AHxJ9h2VCtbQ
zD32E9KmycAigBtomp1KY1Y2X8wXipc9j89u2oU8k1Iwa1A9arvAbws4VBGbHR/0
1YxM3QQrOKCG5gWQxDTLm1JoY205D7bqmYOkHBxE7kj5dos819mxHHLdZQ2g1ytU
rTqR1xHzp2EPv8V3MEhxw4YitdGXWcukoy8Y1JTCjGytSfaV0U8VzK7j0G6/gASB
1SHD67XfNWzFhNRRXP/5TwWeZK1Oe4p9sC25mdHxNRd2Cb21zfPkAOtvBK+hMOWJ
KqEDd9TvP3PLi2bOLTJVZXt5enyxiVby/NtKFMFfxzGsEkVUXEvt0F//xw==
=NmkI
-----END PGP MESSAGE-----
root@portal:/etc/namedb>
```

Рис. 9. Зашифрованное сообщение

Признайтесь, что понять что-либо на рис. 9 сложно.

В бизнесе информация стоит денег, а ее утечка часто означает колоссальные неприятности. Поэтому PGP здесь практически незаменим в определенных ситуациях. Ведь по электронной почте пересылают счета, накладные, договора и другие финансовые документы. И которые вполне можно прочитать с сервера провайдера (рис. 8). Надо отметить, что прикрепленные файлы также изящно «выцепляются» из писем.

Другая опасность: подделка писем. Например, вы получаете от начальника письмо с распоряжением снять деньги со счета. Но где гарантия, что это писал именно он? Поэтому важно подписывать письма с помощью цифровой подписи. У подписанное письма бесполезно менять поле адресата From, т. к. в письме содержится дополнительная информация о адресате и корреспонденте.

3.3. Как работает PGP

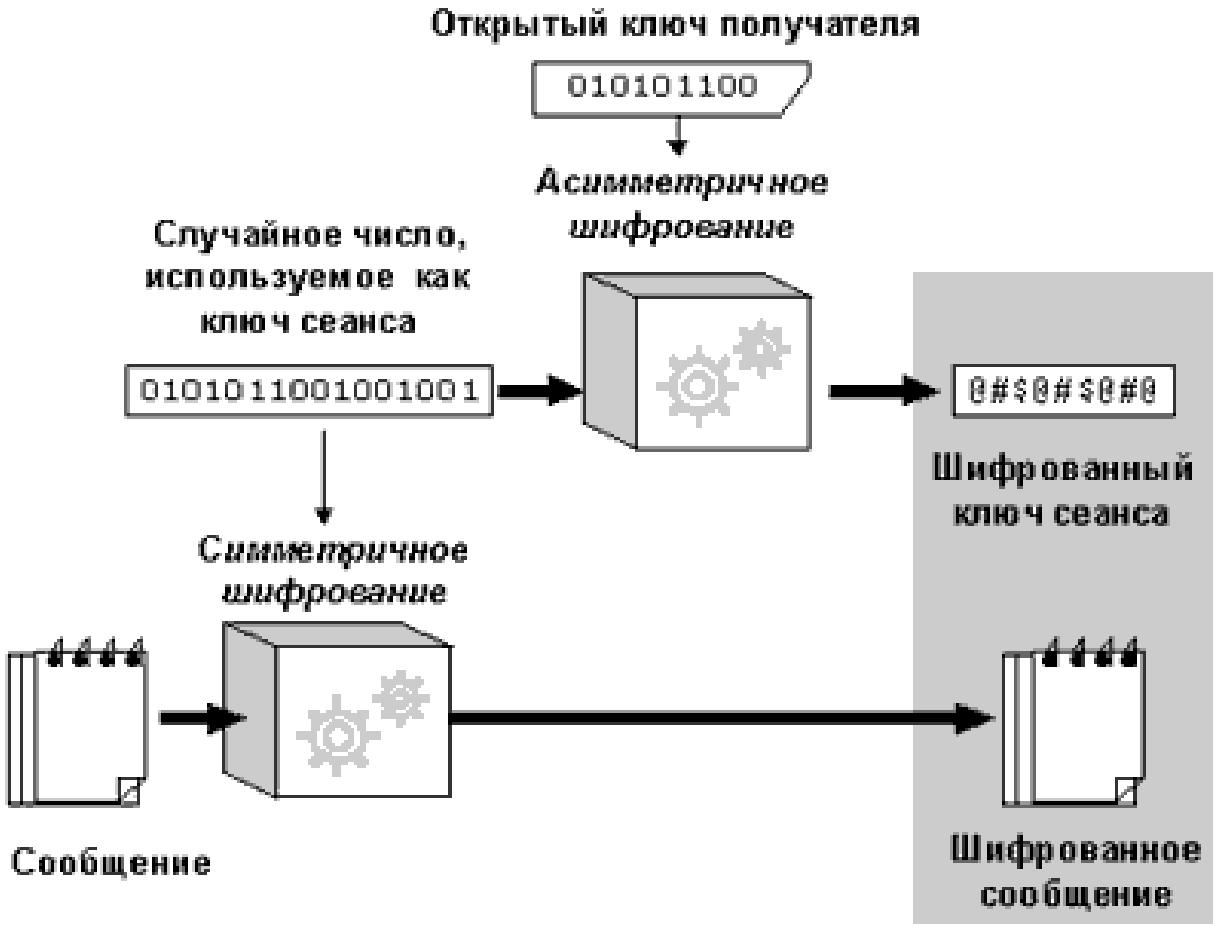

Рис. 10. Схема шифрования в PGP

Когда пользователь шифрует сообщение с помощью PGP, то программа сначала сжимает текст, что сокращает время на отправку со-

общения через модем и увеличивает надежность шифрования. Большинство приемов криптоанализа основаны на исследовании «рисунков», присущих конкретным текстовым файлам, что помогает взломать ключ. Сжатие ликвидирует эти «рисунки» и таким образом повышает надежность зашифрованного сообщения.

Для шифрования сообщения (рис. 10) используется качественный и быстрый алгоритм шифрования с секретным ключом. В ходе процесса, невидимого пользователю, для шифрования открытого текста используется временный случайный ключ, сгенерированный специально для этого «сеанса» (он представляет собой случайное число, созданное за счет движений мышки и нажатий на клавиши клавиатуры).

Затем данный случайный ключ шифруется с помощью открытого ключа получателя. Этот зашифрованный с использованием открытого ключа сеансовый ключ отправляется получателю вместе с зашифрованным текстом.

Как показано на рис. 11, процесс расшифровки происходит в обратном порядке. Личный ключ получателя используется для восстановления временного сеансового ключа, который, в свою оче-

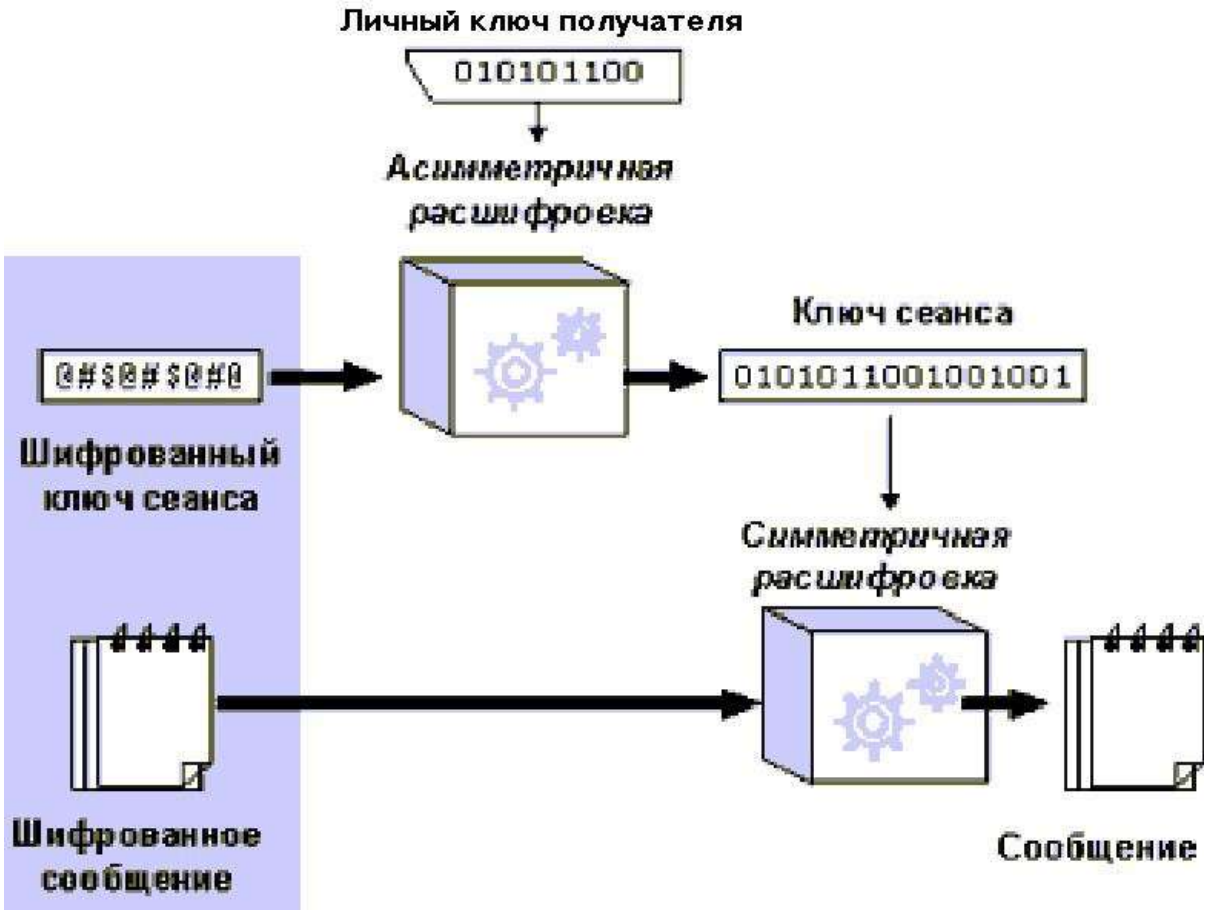

Рис. 11. Схема расшифровки в PGP

редь, используется при запуске быстрого алгоритма с секретным ключом для расшифровки основного тела сообщения.

3.4. Функции PGP

Криптографическая система PGP объединяет удобство шифрования открытым ключом со скоростью работы алгоритма с секретным ключом. Симметричное шифрование почти в тысячу раз быстрее асимметричного. Шифрование открытым ключом, в свою очередь, предоставляет простое решение проблемы распространения ключей и передачи данных. Используемые совместно, скорость исполнения и распространение ключей взаимно дополняются и улучшаются без ущерба безопасности.

Характеристика функций PGP Таблица 1

Функция	Используемые алгоритмы	Описание
1	2	3
Цифровая подпись	DSS/SHA или RSA/SHA	С помощью SHA-1 создается хэш-код сообщения. Хэш-код шифруется личным ключом отправителя с помощью DSS или RSA и включается в сообщение
Шифрование сообщения	CAST либо IDEA, либо «тройной» DES с тремя ключами и алгоритмом Диффи-Хеллмана или RSA	Сообщение шифруется с помощью CAST-128 или IDEA, 3DES с одноразовым сеансовым ключом, генерируемым отправителем. Сеансовый ключ шифруется с помощью алгоритма Диффи-Хеллмана или RSA с использованием открытого ключа получателя и включается в сообщение
Сжатие	ZIP	Сообщение можно сжать для хранения или передачи, используя ZIP
Совместимость на уровне электронной почты	Преобразование в 64-символьный формат	Чтобы обеспечить прозрачность для всех приложений электронной почты, шифрованное сообщение можно превратить в строку ASCII, используя преобразование в 64-символьный формат

Сегментация		Чтобы соответствовать ограничениям максимального размера сообщений, PGP выполняет сегментацию и обратную сборку сообщения

Функциональные возможности PGP складываются из следующих основных сервисов: аутентификация, обеспечение конфиденциальности, сжатия, совместимости на уровни электронной почты, сегментации. Краткая характеристика функций PGP представлена в таблице 1 [4].

3.5. Версии PGP

С сентября 2002 г. поддержкой и развитием Pretty Good Privacy занимается компания PGP Corporation [22].

В настоящее время основными компонентами PGP являются:

- PGPdisk — шифрование данных на жестких дисках;
- PGPkeys — доступ к таблице личных ключей, а также открытых ключей корреспондентов;
- PGPmail — шифрование и расшифровка данных;
- PGPtray — шифрование и расшифровка данных в буфере обмена и управление основными приложениями PGP;
- PGPAdmin — создание криптографической системы для организации;
- PGP ICQ — шифрование текста сообщений ICQ;
- PGP Net — реализация стека протоколов IPSec и IKE.

PGP Corporation выпускает три линии коммерческих продуктов с разной функциональностью — Personal, Workgroup и Enterprise, а также решение для мобильных устройств. Параллельно существует бесплатный вариант PGP Freeware. Во все продукты восьмой версии добавлена поддержка Windows XP и Mac OS X; их исходные коды открыты [20].

PGP — это не только программное обеспечение, но и стандарт [21]. Существует проект PGP International [23], предлагающий свободные версии PGP, PGPdisk, PGPfone (защита телефонных коммуникаций), GNU Privacy Guard. Проект затеян ради преодоления ограничений на экспорт сильной криптографии из США. По сути, PGPi отличается от PGP лишь в деталях — вроде переноса сервера аутенти-

фикации из США в Европу и портирования продукта на экзотические платформы [20].

4-й день. Установка PGP

Довольно с вас. У вас воображенье
В минуту дорисует остальное;
Оно у нас проворней живописца,
Вам все равно, с чего бы ни начать,
С бровей ли, с ног ли.

А.С. Пушкин. Каменный гость

4.1. Где взять PGP

Купить PGP можно на сайте PGP Corporation [22]. Бесплатные версии PGP можно найти на самых разных сайтах Интернета, в частности на сайте Массачусетского технологического института.

Свободные версии PGP доступны для скачивания с сервера проекта PGP International [23].

4.2. Установка

1. Запустите инсталляцию программы PGP: выберите файл **pgpfreeware651int.exe, M2,** в окне **Welcome** (рис. 12) выберите **Next**,

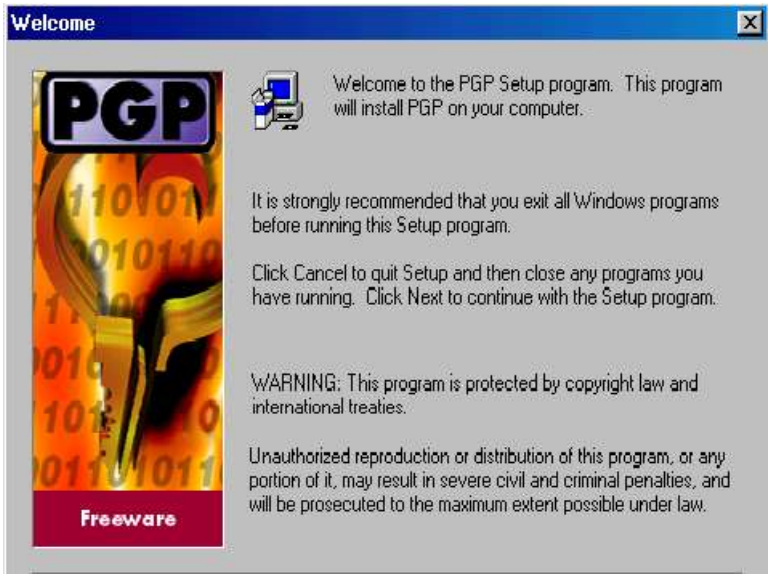

Рис. 12. Окно Welcome

в окне **Software License Agreement** (рис. 13) ознакомьтесь с лицензионным соглашением, выберите **Yes**, выберите **Next**,

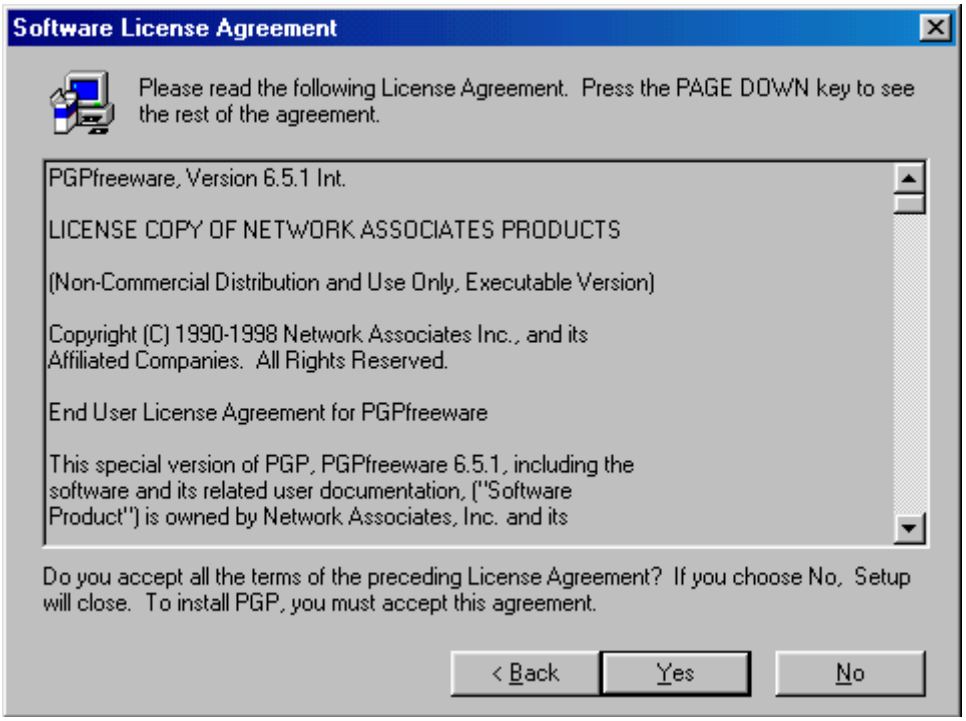

Рис. 13. Окно Software License Agreement

в окне **Important Product Information** (рис. 14) прочитайте новости о PGP, нажмите **Next**,

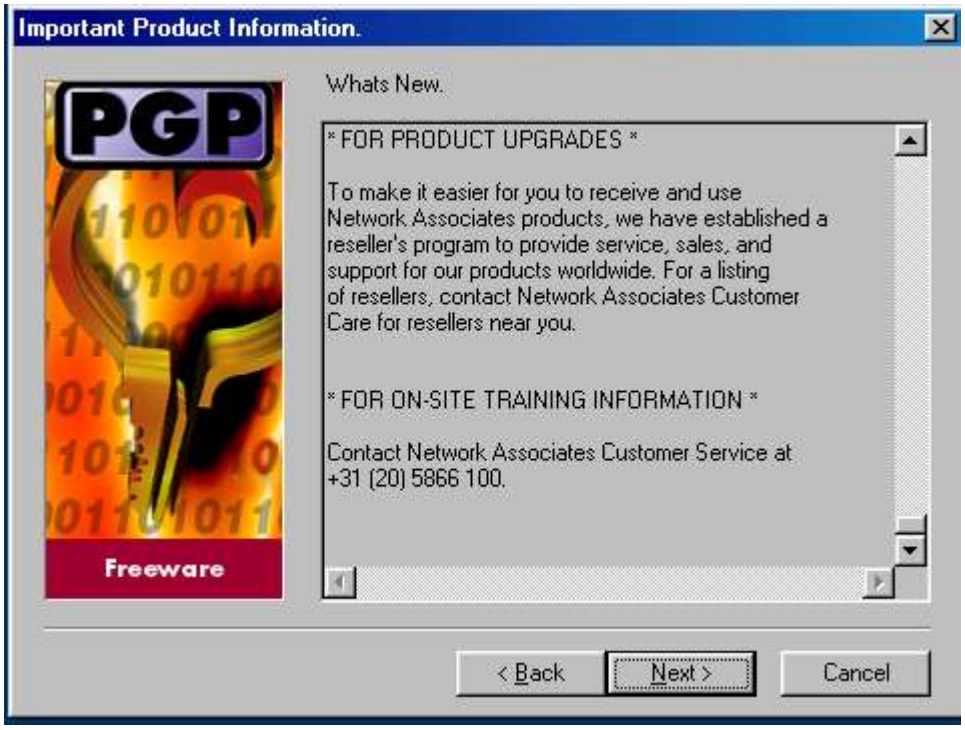

Рис. 14. Окно Important Product Information

в окне **User Information** (рис. 15), в поле **Name** введите **FUB**, в поле **Company** введите **KrasGAU**, нажмите **Next**,

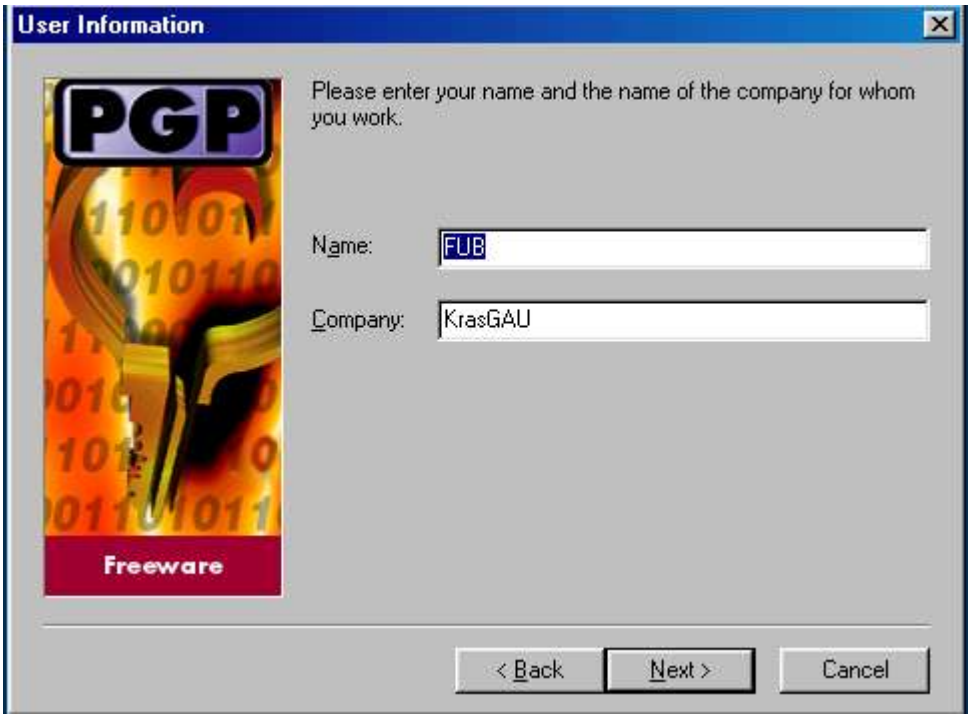

Рис. 15. Окно User Information

в окне **Choose Destination Location** (рис. 16) обратите внимание на папку размещения файлов PGP, если она подходит, нажмите **Next**,

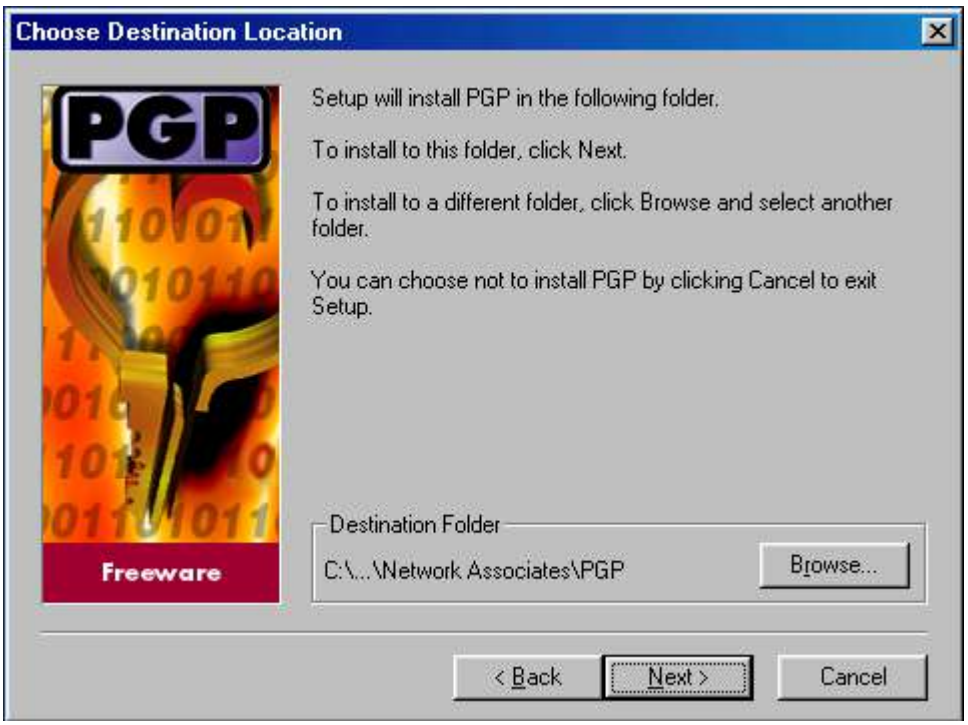

Рис. 16. Окно Choose Destination Location

в окне **Select Components** (рис. 17), выберите установку обязательных файлов **PGP Key Management**, отключите модуль для передачи информации между компьютерами в сети **PGPNet Virtual Private Networking,** отключите модули для почтовых программ **Eudora, Microsoft Exchange/Outlook**, **Microsoft Outlook Express**, нажмите **Next**,

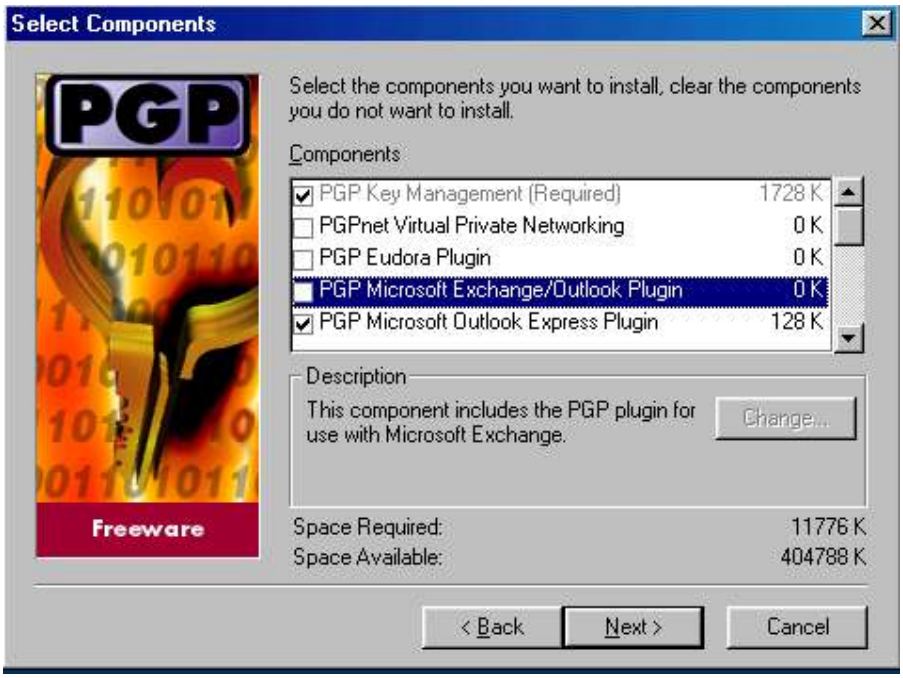

Рис. 17. Окно Select Components

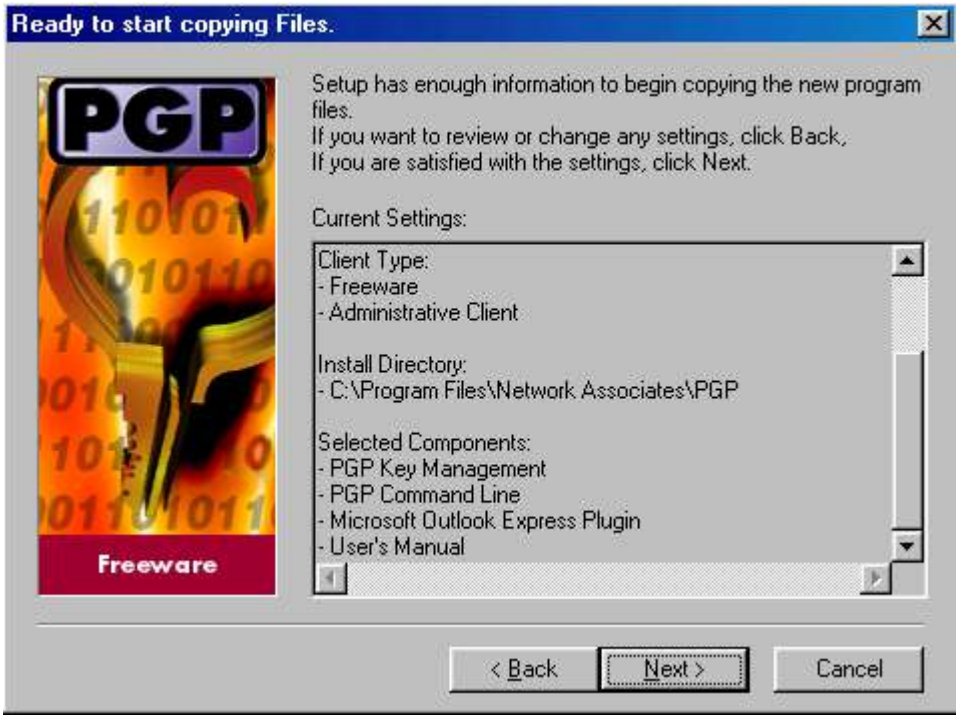

Рис. 18. Окно Ready to start copying Files

в окне **Ready to start copying Files** (рис. 18), просмотрите параметры установки, нажмите **Next,** должно начаться копирование файлов на компьютер.

2. Теперь программа установки спрашивает **Do you have existing keyrings you wish to use**? (нет ли у вас готовых для использования пар ключей?). Такие пары ключей могли быть, если PGP уже была когда-то установлена. При первой установки выберите **Нет.**

3. Программа установки выводит сообщение, что установка завершена и предлагает запустить программу PGPkeys (рис. 19). Пока нам этого не надо, поэтому отключите **Launch PGPkeys** и нажмите **Finish.**

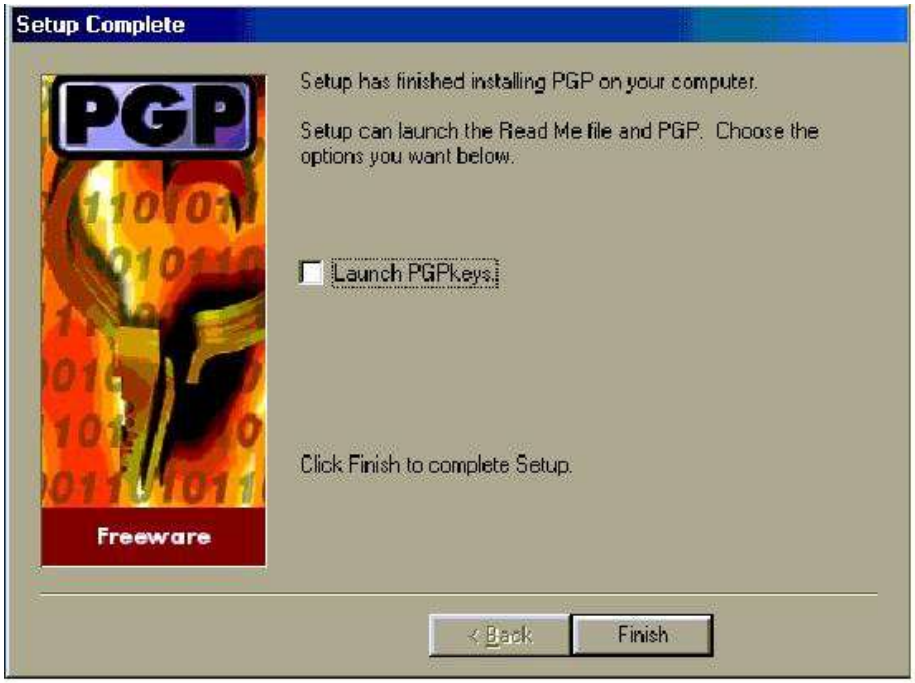

Рис. 19. Окно Setup Complete

4.3. Создание собственной пары ключей

Мы будем использовать шифрование с открытым ключом. Здесь у каждого участника переписки есть пара ключей — public key (открытый ключ, который свободно распространяется среди пользователей PGP) и privacy key (личный ключ, доступ к которому должен иметь только хозяин ключа). Оба этих ключа, открытый и личный, хранятся в файлах, называемых «связками», доступ к которым производится из окна программы PGPkeys.

Ключи хранятся на жестком диске вашего компьютера в зашифрованном состоянии в виде двух файлов: одного для открытых

ключей (pubring.pkr), а другого — для личных (secring.scr). В течение работы с программой PGP вы, как правило, будете вносить открытые ключи ваших корреспондентов в открытые связки. Ваши личные ключи хранятся в вашей личной связке. При потере вашей личной связки вы не сможете расшифровать любую информацию, зашифрованную с помощью ключей, находящихся в этой связке.

Как это работает? Натали посылая сообщение Сереге шифрует его открытым ключом Сергея. Получая сообщение, Серега расшифровывает его своим личным ключом. Никто, кроме получателя, не может расшифровать сообщение, так как никто больше не имеет доступа к его тайному ключу. Даже тот, кто зашифровал сообщение (то есть Натали) с помощью открытого ключа, не сможет его расшифровать.

И наоборот, отвечая Натали, Серега шифрует сообщение открытым ключом Натали. Получая сообщение, Натали расшифровывает его своим личным ключом.

4. Создайте собственную пару ключей с помощью программы Key Generation Wizard: **Пуск | Программы | PGP | PGPkeys,** в поле **Full Name** введите ваше имя и фамилию, например, **Натали Милетто**, в поле **Email address** введите свой электронный адрес, например, **natali@narod.ru**, выберите **Далее** (рис. 20),

Рис. 20. Окно Full Name

выберите тип ключа **Diffie-Hellman/DSS**, выберите **Далее** (рис. 21)**.**

Рис. 21. Окно Key Pair Type

Ключ — это число, которое используется криптографическим алгоритмом для шифрования текста. Как правило, ключи — это огромные числа. Размер ключа измеряется в битах. Число, представленное 1024 битами — очень большое! Несмотря на то, что пара ключей математически связана, практически невозможно из открытого вычислить личный, тем не менее, извлечение личного ключа всегда остаётся возможным, если располагать достаточным временем и вычислительными мощностями. В открытой криптографии, чем больше ключ, тем его сложнее взломать. Уже при размере ключа в 1024 бита самому быстрому компьютеру потребуются, может быть, годы для взлома шифра. Но мощности компьютеров растут, поэтому выберем размер такой, чтобы уж наверняка.

6. Выберите **2048 бит**, выберите **Далее** (рис. 22)**.**

Теперь нужно решить навечно создается пара ключей или на какое-то время? То есть если ключи предполагается использовать лишь временно, например, июнь-август 2004, следует знать, что по истечении этого срока открытый ключ будет негоден для

шифрования предназначенный вам сообщений. Но личный ключ, составляющий пару открытому все равно будет способен расшифровать сообщение.

7. Выберите вечность: **Key pair never expires**, выберите **Далее**.

Рис. 22. Окно Key Pair Size

Теперь очень важный момент: выбор пароля. Парольная фраза — это сочетание нескольких слов, которое теоретически более надежно, чем парольное слово. В виду того, что парольная фраза состоит из нескольких слов, она практически неуязвима против так называемых «словарных атак», где атакующий пытается разгадать ваш пароль с помощью компьютерной программы, подключенной к словарю. Самые надежные парольные фразы должны быть достаточно длинными и сложными и должны содержать комбинацию букв из верхних и нижних регистров, цифровые обозначения и знаки пунктуации. Однако парольная фраза должна быть такой, чтобы ее потом не забыть. Если вы забудете свою парольную фразу, то уже никогда не сможете восстановить свою зашифрованную информацию. Ваш личный ключ абсолютно бесполезен без знания парольной фразы.

8. Придумайте пароль для защиты личного ключа. Этот пароль будет вводится при любом доступе к личному ключу. Нельзя использовать русские или английские слова, которые с помощью

словаря легко подобрать, нельзя использовать имена детей, дружка, клички собак, дни рождения, телефоны.

9. В поле **Passphrase** введите свой пароль, например, **ЯлюблюРозовыеОблака!**

Обратите внимание, что PGP старается вам помочь и по мере ввода символов пароля удлиняется полоска Passphrase Quality — чем она длиннее, тем лучше пароль.

10. Введите тот же пароль **ЯлюблюРозовыеОблака!** в поле **Confirmation**, выберите **Далее** (рис. 23), должен начаться процесс создания пары ключей.

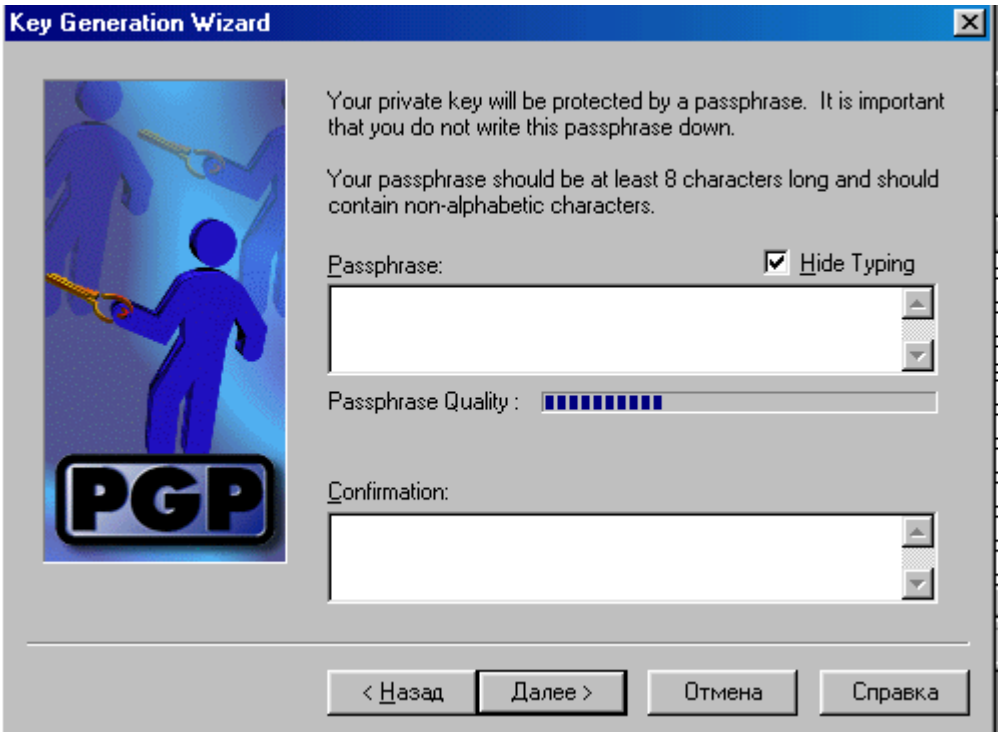

Рис. 23. Окно Passphase

11. Если вы ввели неадекватный пароль, может появиться соответствующее сообщение и для продолжения вы должны, либо подтвердить использование неудачного пароля, либо ввести новый пароль.

12. Если PGP не располагает достаточным для генерации ключа количеством случайных чисел, появится окно **Случайные числа** (PGP Random Data). В этом случае, вы должны подвигать мышью и понажимать на клавиши клавиатуры, пока полоса индикации состояния не заполнится до конца. Движения мыши и нажатия клавиш генерируют случайную информацию, необходимую для создания пары ключей.

13. После вычисления пары ключей и записи их на диск нажмите **Далее** (рис. 24).

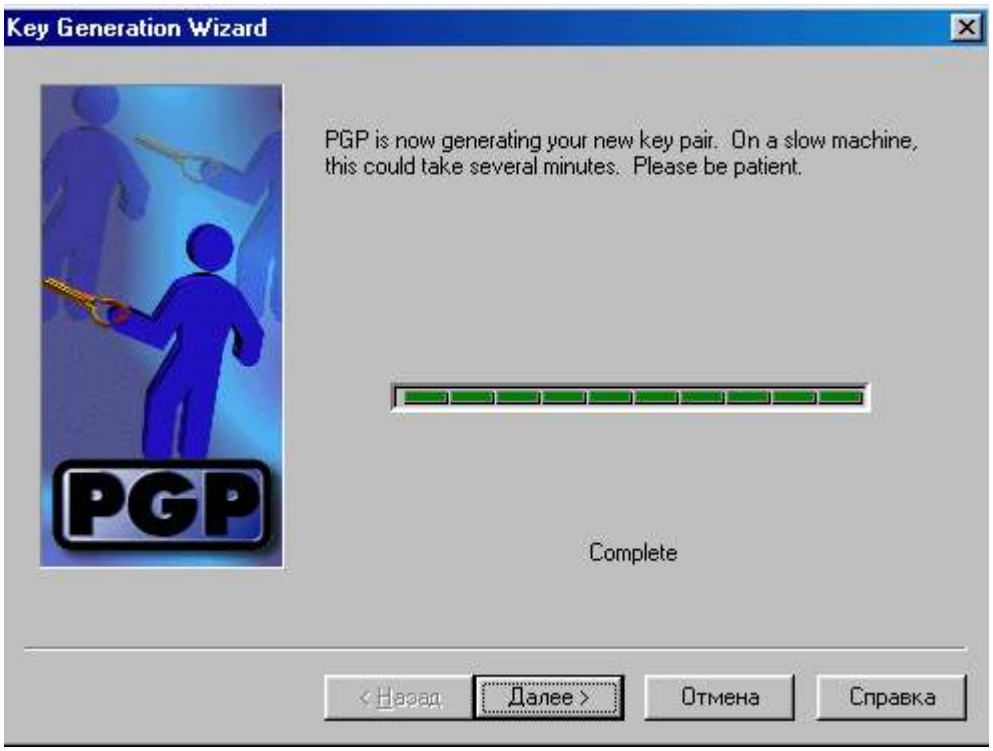

Рис. 24. Окно Complete

14. Далее будет предложено — **Send my key to the root server now** (передать открытый ключ на сервер) — с помощью флажка откажитесь от этого, нажмите **Далее** (рис. 25), нажмите **Готово**.

Рис. 25. Окно Send key to server

4.3. Защита ключей

После создания пары ключей, желательно сделать резервную копию и спрятать ее в надежное место.

15. Создайте копию ключей: выберите **File | Exit**, выберите **Save Backup Now**, в поле **Папка** выберите свою личную папку, в поле **Имя файла** введите имя файла открытого ключа **pubring**, нажмите **Сохранить**, в поле **Имя файла** введите имя файла личного ключа **secring**, нажмите **Сохранить**.

5-й день. Шифрование

> Неизвестность о судьбе Марьи Ивановны пуще всего меня мучила. Где она? Что с нею? Успела ли спрятаться? Надежно ли ее убежище?..
>
> *А.С. Пушкин. Капитанская дочка*

5.1. Панель инструментов PGPkeys

16. Запустите программу PGPkeys: выберите **Пуск | Программы | PGP | PGPkeys.**

Панель инструментов обеспечивает быстрый доступ к часто выполняемым задачам. Вы можете показывать или скрывать панель, используя команду меню View | Toolbar. В таблице 2 показаны элементы стандартной панели.

Элементы стандартной панели PGPkeys Таблица 2

	Generate new keypair — создание новой пары ключей
	Revoke the selected item — отзыв выбранного ключа
	Sign the selected item — подпись выбранного ключа
	Delete the selected item — удаление выбранного ключа
	Open key search window — поиск ключа в списке
	Send key to server — отправка ключа на сервер
	Update key from server — получение ключа с сервера
	Show key or certificate properties — просмотр параметров ключа
	Import key from a file — импорт ключа из файла

	Export selected keys to a file — экспорт выбранного ключа в файл

5.2. Распространение открытого ключа

После создания пары ключей, открытый ключ нужно сделать доступным для других людей, чтобы они смогли шифровать направляемую вам почту или файлы.

Для распространения открытого ключа у вас есть ряд возможностей: отправить копию своего открытого ключа на сервер открытых ключей [15], включить копию открытого ключа в почтовое сообщение, экспортировать открытый ключ в текстовый файл.

17. Будем размещать открытые ключи и зашифрованные файлы в сетевой папке **serverPGP.**

18. Экспортируйте открытый ключ в файл: выберите свой ключ, например, **Милетто**, выберите **Keys | Export**, в поле **Имя файла** введите свое имя, например, **Милетто**, в поле **Папка** выберите **serverPGP**, выберите **Сохранить**.

5.3. Получение открытых ключей

Для того, чтобы отправлять другим пользователям шифрованную почту или файлы, вам необходимо получить копии их открытых ключей. Для этого у вас есть ряд возможностей: взять ключ на сервере открытых ключей [15], взять ключ из тела почтового сообщения, импортировать ключ из файла.

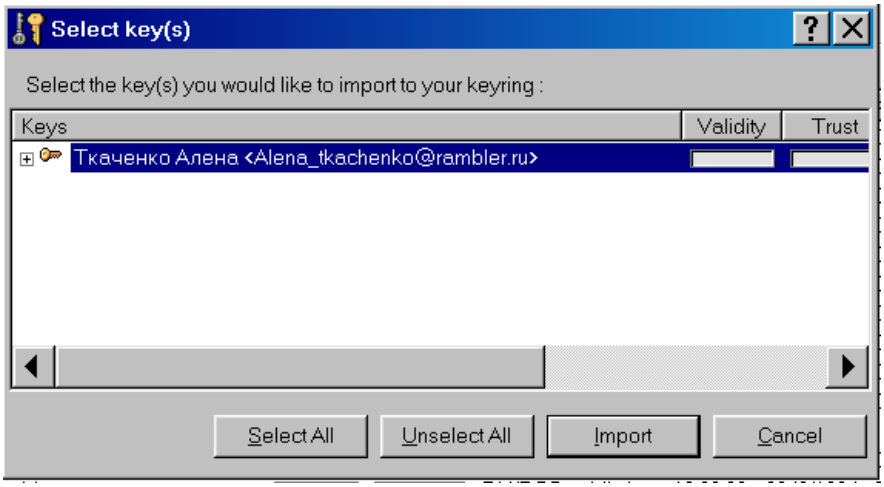

Рис. 26. Окно Select key(s)

19. В окне PGPkeys удалите все ключи, кроме **своего** и **Зиммермана**.

20. Импортируйте ключ товарища из файла: выберите **Keys** | **Import**, в поле **Папка** выберите **serverPGP**, выберите файл товарища, например, **Ткаченко**, выберите **Открыть**, в окне **Select key(s)** (рис. 26) выберите **Import**, в окне PGPkeys должен появиться новый ключ.

5.4. Шифрование через буфер обмена

20. Создайте файл с секретным сообщением своему товарищу (рис. 27).

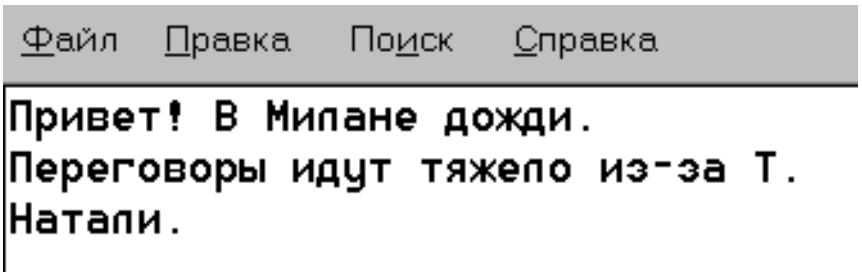

Рис. 27. Окно Блокнота с текстом

21. Перенесите секретный текст в буфер: выберите **Правка** | **Выделить все**, выберите **Вырезать**.

22. Запустите PGPtray: выберите **Пуск | Программы | PGP | PGPtray,** в области индикаторов панели задач должен появится **замочек**.

23. Зашифруйте сообщение: на панели задач выберите **замочек**, выберите **Clipboard** | **Encrypt**, должно появится окно с доступными вам открытыми ключами (рис. 28), выберите ключ получателя, например, **Ткаченко Алена**, перетащите ключ в нижнее окно **Recipients** (Получатели), нажмите **ОК**.

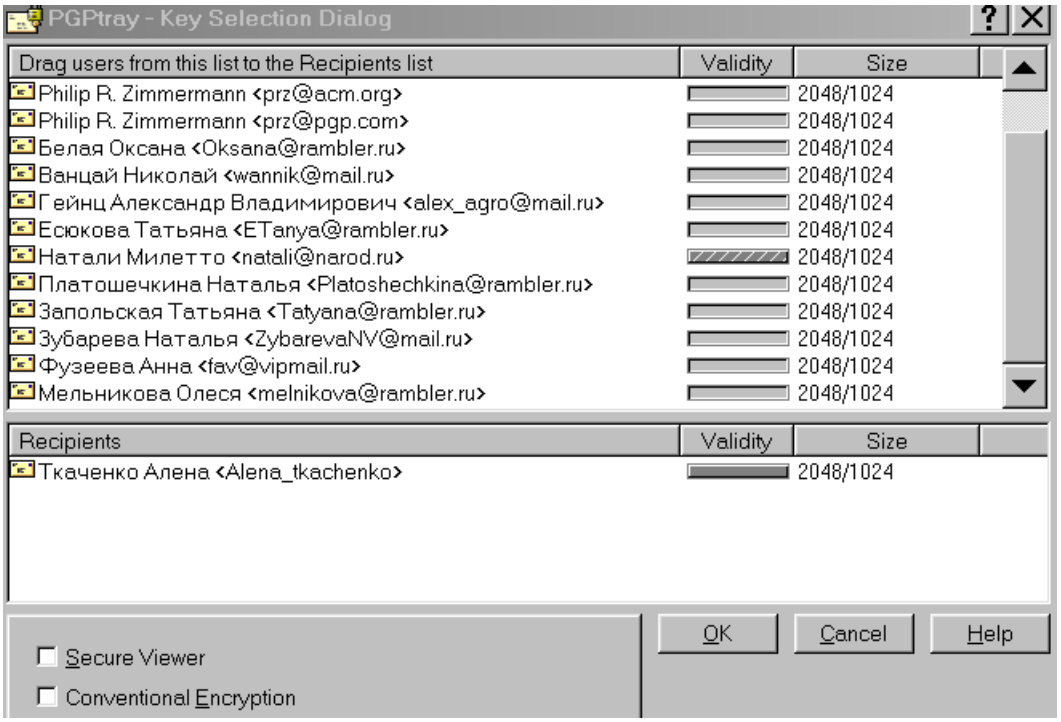

Рис. 28. Окно Key Selection Dialog

24. Вставьте зашифрованное сообщение в файл: выберите **Правка | Вставить,** должна появиться абракадабра (рис. 29).

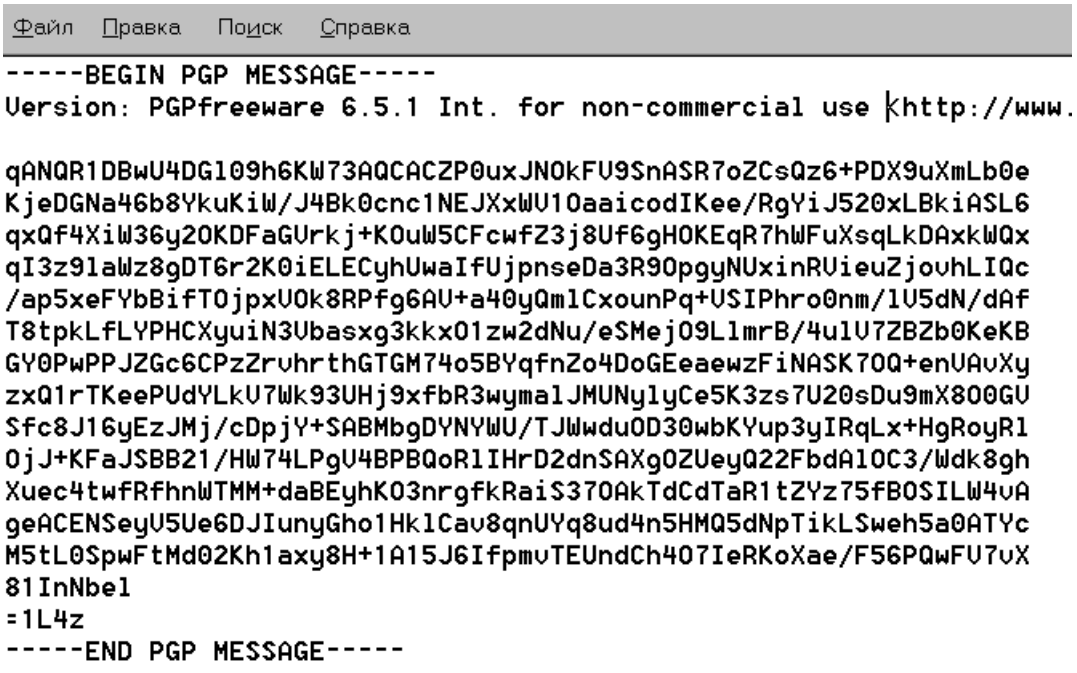

Рис. 29. Окно Блокнота с зашифрованным текстом

25. Сохраните зашифрованное сообщение в файле: выберите **Файл | Сохранить как**, в поле **Папка** выберите **serverPGP**, в поле **Имя файла** введите **ДляТкаченко.txt**.

5.5. Расшифровка через буфер обмена

26. Скопируйте предназначенный вам файл, например, **ДляМилетто.txt,** из папки **serverPGP** в папку **Мои документы.**

27. Скопируйте зашифрованное сообщение в буфер: выберите файл **ДляМилетто.txt, M2,** выберите **Правка | Выделить все**, выберите **Скопировать**.

28. Расшифруйте сообщение: выберите **замочек**, выберите **Clipboard | Decrypt/Verife**, в поле **Enter passphrase for your private key** введите пароль защищающий ваш личный ключ, например, **ЯлюблюРозовыеОблака!**, в окне **Text Viewer** должно появиться посланное вам сообщение.

5.6. Функции PGPtray

PGPtray активизирует замочек и предоставляет лёгкий путь шифрования информации, содержащейся в буфере обмена.

29. Просмотрите основные параметры PGP: на панели задач выберите **замочек**, **МП**, выберите **Options**, выберите вкладку **General**.

Если опция **Always encrypt to default key** включена — то все данные, зашифрованные открытым ключом получателя, будут шифроваться также и вашим основным ключом.

Опция **Faster key generation** — ускоренное создание ключа — позволяет несколько сэкономить драгоценное время, хотя теоретически и снижает надёжность ключа.

Опция **Cache decryption passphrases for** — кэшировать пароль для расшифровки в течение указанного времени. Если при чтении огромного вороха корреспонденции установить время кэширования побольше, тогда не придётся всякий раз, по истечении данного срока, набирать парольную фразу. Но надо помнить об опасности такого решения, поскольку на время кэширования ваш пароль доступен для перехвата взломщиками.

Опция **Cache signing passphrases for** — кэшировать пароль для подписи в течение указанного времени. Эта опция упрощает подпись документов.

30. Выберите вкладку **Files**, на которой можно менять место расположения связок ключей.

31. Выберите вкладку **Email**, которая предназначена для установления предпочтений при работе с электронной почтой.

Здесь вы можете изменять параметры работы с почтой для программ, поддерживаемых с помощью встраиваемых модулей. Если отметить галочками все строки, это сократит в дальнейшем перечень процедур при работе с шифрованными почтовыми сообщениями.

Обратите внимание, что по умолчанию задаётся количество знаков в одном столбце подписываемого сообщения. Это вызвано тем, что разные почтовые программы по-разному сворачивают текст, отсутствие принудительной стандартизации может разрушить структуру подписанного сообщения и привести к невозможности подтверждения подписи.

32. Выберите вкладку **Servers**, которая содержит адреса серверов, на которых хранятся ваши открытые ключи.

33. Выберите вкладку **CA**, которая предназначена для настройки работы с сертифицирующими органами, которые выдают цифровые сертификаты.

34. Выберите вкладку **Advanced**, которая содержит перечень используемых алгоритмов шифрования и моделей доверия.

Все остальные команды в **PGPtray** предназначены для работы с данными, размещёнными в буфере обмена (**Clipboard**) или с **выделенными** данными в текущем окне (**Current Window**). Вот список этих команд:

Empty — очистить буфер обмена от старого содержимого;

Edit — работа в простейшем текстовом редакторе;

Decrypt & Verify — расшифровать и идентифицировать информацию;

Encrypt & Sign — зашифровать и подписать данные;

Sign — подписать сообщение;

Encrypt — зашифровать сообщение.

5.7. Шифрование и расшифровка в Проводнике

35. Создайте файл, например, **ДляФузеевой.txt,** с текстом своему товарищу.

36. Зашифруйте файл: **Пуск** | **Программы** | **Проводник**, выберите созданный вами файл **ЧтениеФузеевой.txt**, **МП**, в контекстном меню выберите **PGP** | **Encrypt**, выберите ключ получателя, например, **Фузеева Анна**, перетащите ключ в нижнее окно **Recipients** (Получатели), нажмите **ОК**.

37. Скопируйте файл **ДляФузеевой.txt.pgp** в папку **serverPGP.**

38. Скопируйте предназначенный вам файл, например, **ДляМилетто.txt.pgp,** из папки **serverPGP** в папку **Мои документы**.

39. Расшифруйте файл: выберите файл **ДляМилетто.txt.pgp**, **М2**, в поле **Enter passphrase for your private key** введите пароль защищающий ваш личный ключ, например, **ЯлюблюРозовыеОблака!,** нажмите **Сохранить,** в Проводнике должен появиться файл с расшифрованным текстом.

40. Просмотрите сообщение: выберите файл, например, **ДляМилетто.txt, М2,** прочитайте посланное вам сообщение.

5.8. Шифрование в почтовой программе

PGP включает встроенные модули для почтовых клиентов MS Outlook, Outlook Express, Eudora, Apple Mail, Entourage. Большинство пользователей обращаются к PGP непосредственно из рабочего окна почтового клиента, в меню которого появляется дополнительный пункт PGP, с доступом к криптографическим функциям.

Если же используется почтовый клиент, не поддерживаемый PGP посредством встроенных модулей или этот модуль не был установлен при инсталляции, то для шифрования надо использовать буфер обмена.

41. Составьте секретное сообщение: выберите **Пуск | Программы | Outlook Express** | **Создать**, введите текст.

42. Перенесите секретный текст в буфер: выберите **Правка** | **Выделить все**, выберите **Вырезать**.

43. Запустите PGPtray: выберите **Пуск | Программы | PGP | PGPtray,** в области индикаторов панели задач должен появится **замочек**.

44. Зашифруйте сообщение: на панели задач выберите **замочек,** выберите **Clipboard** | **Encrypt**, должно появится окно с доступными вам открытыми ключи, выберите ключ получателя, например,

Ткаченко Алена, перетащите ключ в нижнее окно **Recipients** (Получатели), нажмите **ОК**.

45. Вставьте зашифрованное сообщение: выберите **Правка** | **Вставить,** должна появиться абракадабра.

46. Сообщение можно отправлять: выберите **Файл** | **Отправить позже**.

6-й день. Цифровая подпись

На первом листике встречаешь
Qu ecrirez-vous sur ces tablettes;
И подпись: t. a. v. Annette;
А на последнем прочитаешь:
«Кто любит более тебя,
Пусть пишет далее меня».

А.С. Пушкин. Евгений Онегин

6.1. Отпечаток

Любой человек, который пожелает сообщить вам нечто секретное, должен иметь ваш открытый ключ. И чтобы не пересылать свой ключ каждому собеседнику, лучше поместить его в общее хранилище (например, в папку serverPGP), где он будет доступен всем желающим. Но одно из наиболее уязвимых мест шифрования с открытым ключом — возможность того, что противник (конкурент, шпион, бывшая подружка) предпримет атаку с активной ретрансляцией (a «man-in-the-middle» attack).

Представим себе, что Натали хочет послать шифрованное сообщение Серёге. Для этого она посещает сервер открытых ключей, отыскивает там открытый ключ Серёги, шифрует им сообщение и посылает его электронной почтой. Пока все хорошо. Но вот беда, этот же сервер открытых ключей посетила некто Т*, которая подменила открытый ключ Серёги своим собственным открытым ключом. После подмены Т* перехватывает сообщение для Серёги, расшифровывает его своим личным ключом, изучает письмо, копирует в свой архивчик, а затем снова шифрует его подлинным открытым ключом Серёги и отсылает по назначению. Фактически все это может делать компьютерная программа, установленная по пути следования электронной почты.

То есть ни в коем случае нельзя позволять подменять открытые ключи. Но как? У каждого открытого ключа есть так называемый **отпечаток** (fingerprint). Если отпечаток вашей копии открытого ключа и копии подлинника совпадают (для этого можно попросить хозяина ключа продиктовать отпечаток по телефону) — то вы располагаете подлинной копией. Некоторые с этой целью помещают отпечатки ключей на свои визитные карточки. .

47. Выберите **Пуск | Программы | PGP | PGPkeys,** просмотрите общие атрибуты ключей расположенные вдоль верха окна: **Keys, Validity, Trust, Size, Description.**

Validity (действительность) — отображает степень уверенности в том, что ключ принадлежит номинальному владельцу. Действительность ключа вычисляется исходя из того, кто сертифицировал ключ. Открытый ключ, который вы сертифицировали сами, обладает наибольшим уровнем действительности. Если ключ не сертифицирован никакими подписями, он рассматривается как недействительный.

Trust (надежность) — указывает уровень доверия, которое вы присвоите владельцу ключа в смысле его способности быть посредником при сертификации ключей третьих лиц.

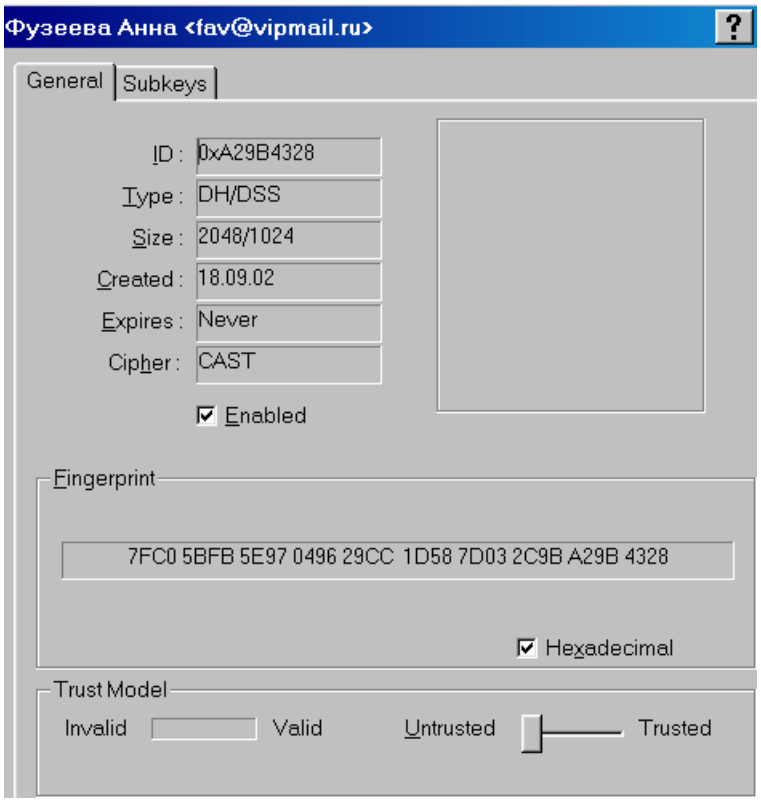

Рис. 30. Окно Key Properies

48. Просмотрите отпечаток ключа: выберите ключ товарища, например, **Фузеева Анна**, выберите **Keys | Properties | Fingerprint,** где 7FC0 5BFB 5E97 0496 29CC 1D58 7D03 2C9B A29B 4328 — уникальный идентификационный номер, создаваемый при создании пары ключей и являющийся средством контроля подлинности ключа (рис. 30).

6.2. Подпись

Отпечаток ключа это неплохо. Однако, часто не известен ни телефон хозяина ключа, ни его голос. В этом случае спасает **цифровая подпись.**

Огромным преимуществом криптографии с открытым ключом является возможность использования цифровой подписи, которая позволяют получателю сообщения удостовериться в личности отправителя сообщения, а также в целостности полученного сообщения. Цифровая подпись исполняет ту же самую функцию, что и ручная подпись с помощью гусиного пера. Однако ручную подпись легко подделать. Цифровую же подпись подделать почти невозможно.

Важное преимущество использования PGP состоит в том, что при цифровой подписи PGP применяет так называемую хэш-функцию, которая действует таким образом, что в случае изменения информации, пусть даже на один бит, результат хэш-функции будет совершенно иным.

Дайджест сообщения — это 160- или 128-битная криптографически стойкая односторонняя хэш-функция. В чем-то она похожа на «контрольную сумму» или код проверки ошибок CRC, который компактно представляет сообщение и используется для проверки сообщения на наличие изменений. В отличие от CRC, дайджест сообщения формируется таким образом, что злоумышленник не может сгенерировать поддельное сообщение с аналогичным дайджестом. Дайджест сообщения передается в зашифрованном личным ключом отправителя виде, составляя цифровую подпись сообщения. При получении сообщения получатель использует PGP для восстановления исходных данных и проверки подписи.

При условии использования надежной формулы хэш-функции невозможно вытащить подпись из одного документа и вложить в другой, либо каким-то образом изменить содержание сообщения. Любое изменение подписанного документа сразу же будет обнаружено при проверке подлинности подписи.

Итак, как же лишить таинственную Т* возможности читать чужие сообщения? Для этого между Натали и Серёгой состоялась тайная встреча, во время которой они обменялись открытыми ключами. Зная друг друга в лицо, они считают полученные ключи подлинными. И поэтому оба, придя домой, подписывают ключи — Натали

подписывает открытый ключ Серёги своим личным ключом, Серёга подписывает открытый ключ Натали своим личным. Теперь чтобы подменить открытый ключ Сергея, Т* должна подделать подпись Натали, а для этого ей нужен личный ключ Натали. Но у Т* такой возможности нет! Если даже она проникнет в компьютер Натали и утащит ее личный ключ — она не сможет им воспользоваться, так как не знает пароля.

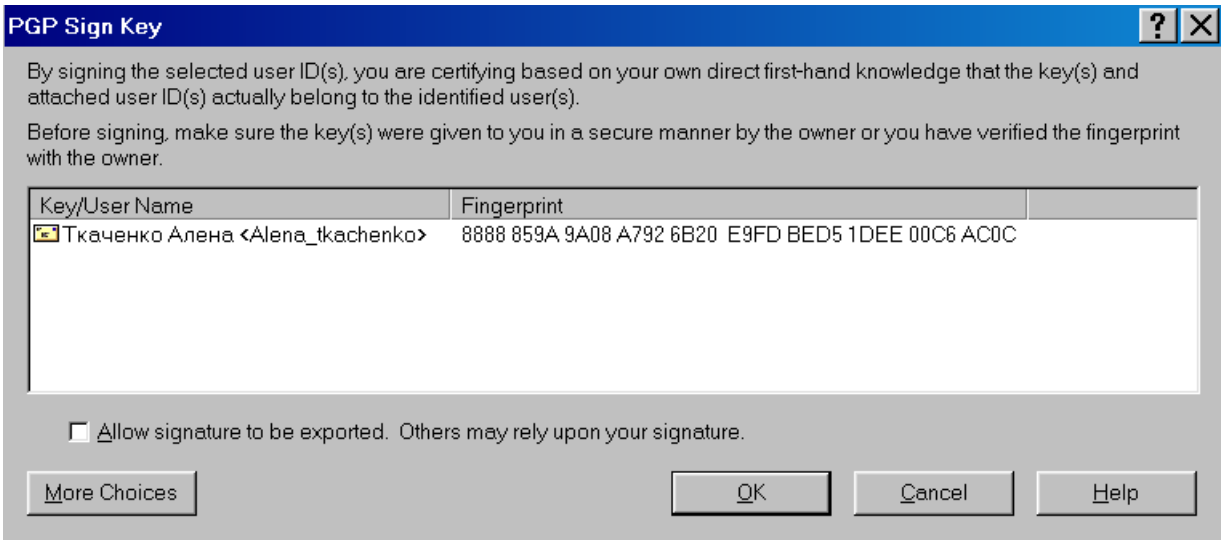

Рис. 31. Окно PGP Sign Key

49. Подпишите ключ: выберите ключ своего товарища, например, **Ткаченко Алена**, **МП**, выберите **Sign**, появляется окно **PGP Sign Key** (рис. 31) в котором показан цифровой отпечаток ключа Алёны и высвечивается предупреждение: подписывая ключ, вы основываетесь на достоверном знании того, кому он принадлежит и свидетельствуете, что верны также имя и почтовый адрес владельца ключа, нажмите **ОК**, далее в поле **Passphrase of signing key** введите свой пароль для защиты личного ключа, например, **ЯлюблюРозовыеОблака!,** нажмите **ОК**.

Рис. 32. Окно PGPkeys

50. Обратите внимание, что в графе **Validity** вместо **пустого** прямоугольника кружка появился **заполненный** прямоугольник, что говорит о возросшем доверии к ключу (рис. 32).

6.3. Схемы цифровой подписи

На рис. 33 показано, как генерируется цифровая подпись.

Получатель может проверить правильность цифровой подписи, используя открытый ключ отправителя для расшифровки дайджеста сообщения (рис. 34). Это доказывает, что тот, кто указан в качестве отправителя сообщения, является его создателем и что сообщение не было впоследствии изменено другим человеком, так как только отправитель владеет своим закрытым ключом, использованным для формирования цифровой подписи. Подделка цифровой подписи невозможна, и отправитель не может впоследствии отрицать ее подлинность.

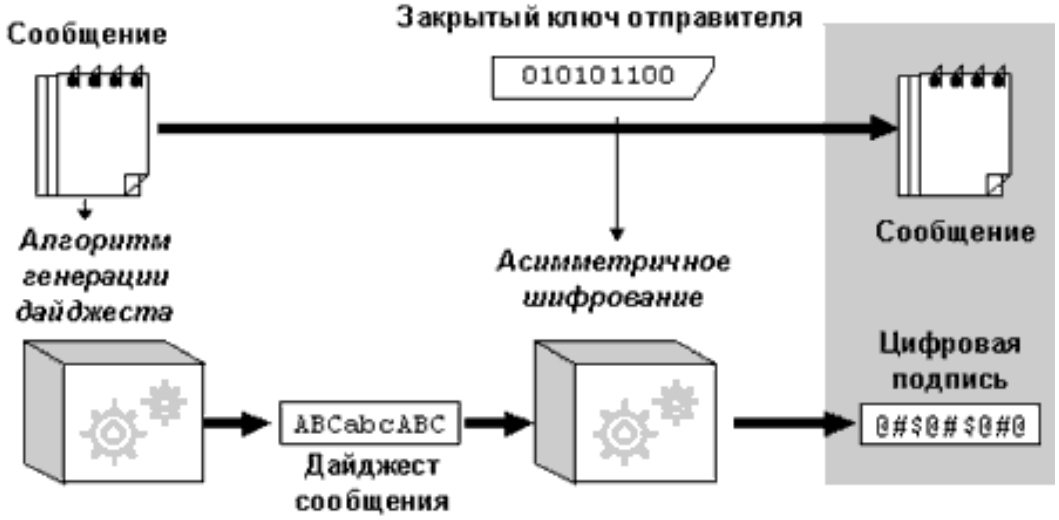

Рис. 33. Схема генерации цифровой подписи

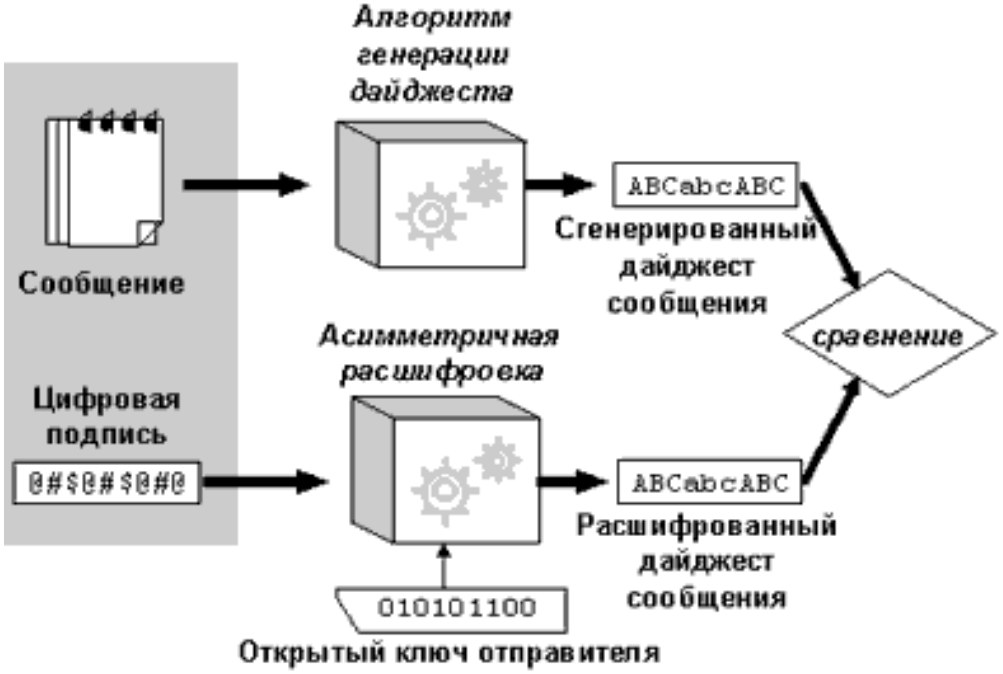

Рис. 34. Проверка цифровой подписи

6.4. Цифровая подпись через буфер обмена

Цифровая подпись позволяет защитить электронный документ от подделки гораздо надежнее, чем обычная подпись и печать, которые подделываются нынче совсем просто.

51. Создайте файл с секретным сообщением своему товарищу (рис. 35).

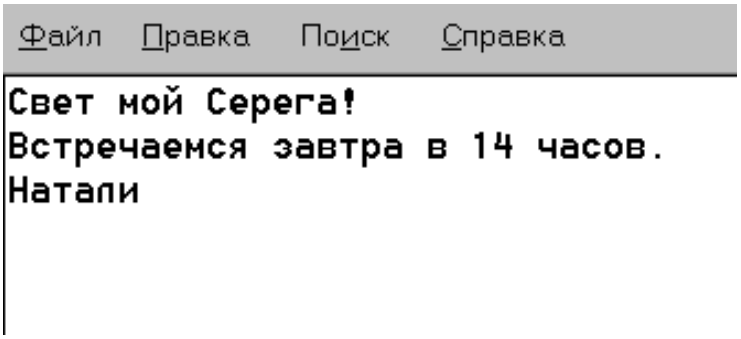

Рис. 35. Сообщение в Блокноте

52. Перенесите сообщение в буфер обмена: выберите **Правка** | **Выделить все**, выберите **Вырезать**.

53. Подпишите сообщение: в правом нижнем углу экрана выберите **замочек**, выберите **Clipboard** | **Sign**,

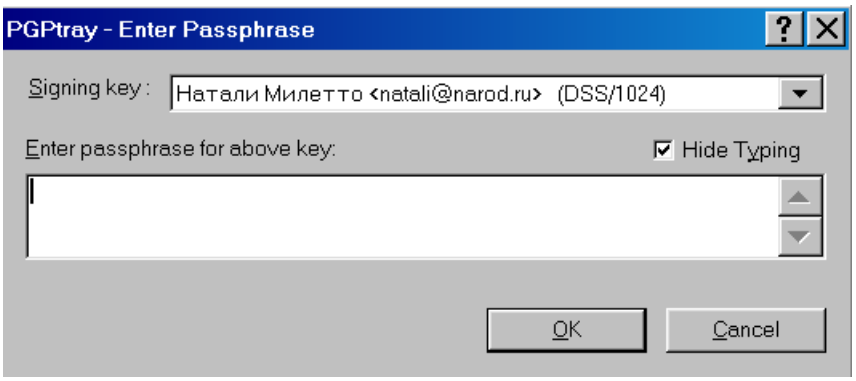

Рис. 36. Окно Enter Passphrase

в поле **Signing key** должен быть ваш ключ, в поле **Enter passphrase for above key** (рис. 36) введите ваш пароль для тайного ключа, например, **ЯлюблюРозовыеОблака!,** нажмите **ОК**.

54. Вставьте зашифрованный текст в файл: выберите **Правка** | **Вставить,** должно появиться ваше сообщение и цифровая подпись (рис. 37), которая начинается словами BEGIN PGP SIGNATURE и заканчивается END PGP SIGNATURE.

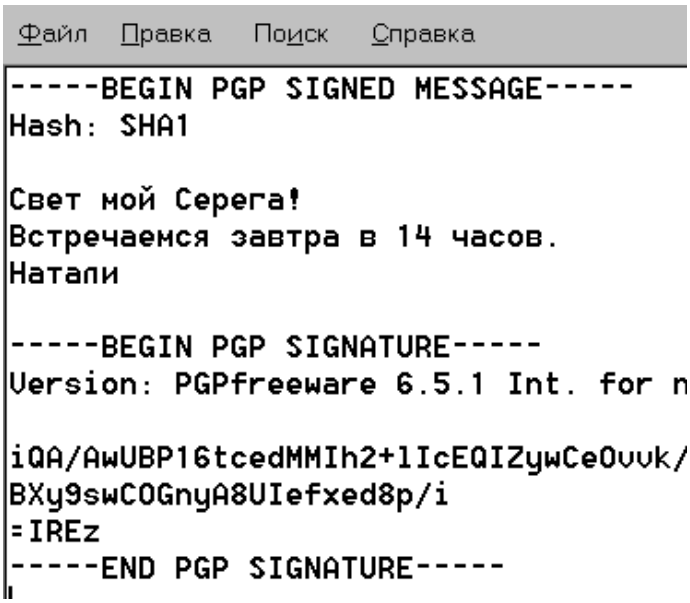

Рис. 37. Подписанное сообщение в Блокноте

55. Проверьте сообщение: выберите **Правка** | **Выделить все**, выберите **Копировать**, выберите **замочек**, выберите **Clipboard** | **Decrypt/Verife**, на экране должно появиться подписанное вами сообщение, а также сведения о подписи: кто подписал, когда подписал, когда проверили, и далее результат проверки — **PGP signature status: good** (рис. 38) — эти слова говорят о правильности подписи, нажмите **OK**.

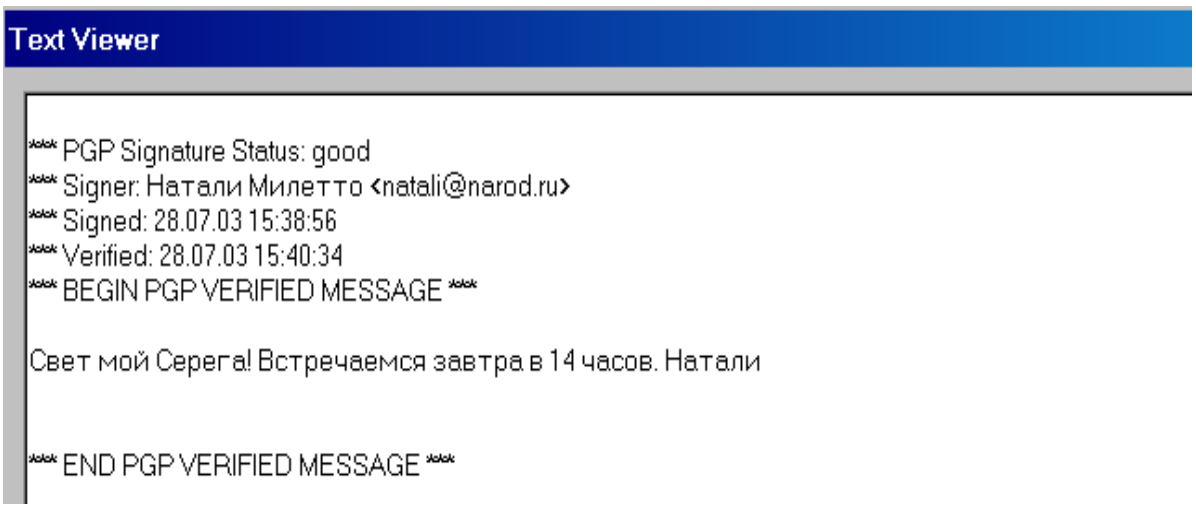

Рис. 38. Окно Viewer

56. Измените сообщение: например, уберите в секретном тексте восклицательный знак после слова **Серега**.

57. Проверьте сообщение: выберите **Правка** | **Выделить все**, выберите **Копировать**, выберите **замочек**, выберите **Clipboard** | **Decrypt/Verife**, на экране должно появиться подписанное вами

сообщение, но — **PGP signature status: bad** (рис. 39) — говорит, что подпись и документ не соответствуют друг другу, нажмите **OK**.

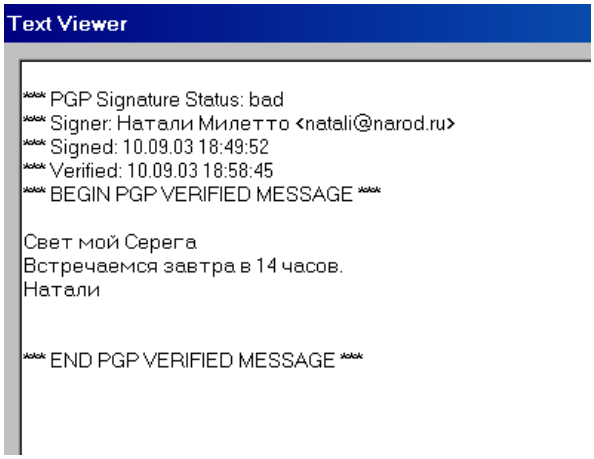

Рис. 39. Окно Viewer

6.5. Шифрование и цифровая подпись в Проводнике

58. Создайте файл, например, **ДляЗубаревой.txt,** с секретным сообщением своему товарищу.

59. Зашифруйте и подпишите файл: **Пуск** | **Программы** | **Проводник**, выберите созданный файл **ДляЗубаревой**, **МП**, выберите **PGP** | **Encrypt&Sign**, выберите ключ получателя, например, **Зубарева Наталья**, перетащите ключ в нижнее окно **Recipients** (Получатели), нажмите **ОК**, в поле **Signing key** должен быть ваш ключ, в поле **Enter passphrase…** введите ваш пароль для тайного ключа, например, **ЯлюблюРозовыеОблака!,** нажмите **ОК**.

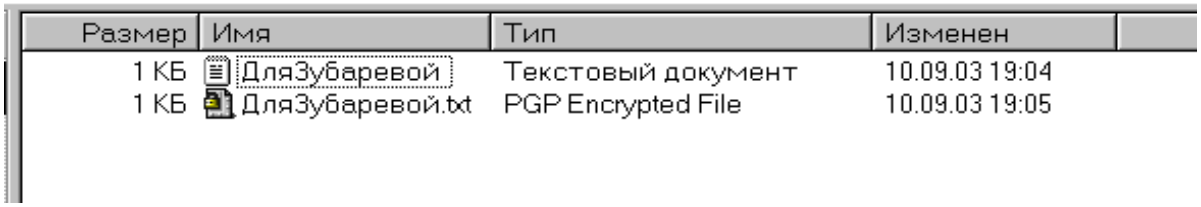

Рис. 40. Окно Проводника

60. Скопируйте зашифрованный файл **ДляЗубаревой.txt.pgp** (рис. 40) в папку **serverPGP.**

61. Скопируйте предназначенный вам файл, например, **ДляМилетто.txt.pgp,** из папки **serverPGP** в папку **Мои документы.**

62. Расшифруйте файл: выберите предназначенный вам файл, например, **ДляМилетто.txt.pgp**, **М2**, в поле **Enter passphrase…** введите пароль защищающий ваш личный ключ, например,

ЯлюблюРозовыеОблака!, нажмите **Сохранить**, в Проводнике должен появиться файл с расшифрованным текстом.

63. Просмотрите сообщение: выберите файл, например, **ДляМилетто.txt, M2,** прочитайте посланное вам сообщение.

7-й день. Управление ключами

Лампады тихий свет
Бледнел пред утренней зарею,
И утро веяло в темницу. И поэт
К решетке поднял важны взоры…
Вдруг шум. Пришли, зовут. Они!
Надежды нет!
Звучат ключи, замки, запоры.
Зовут…

А.С. Пушкин. Андрей Шенье

7.1. Связка ключей

64. Запустите программу PGPkeys: выберите **Пуск | Программы | PGP | PGPkeys.**

Ключи, которые вы создаете, а также открытые ключи, получаемые от других, хранятся в связках, которые представляют собой файлы на жестком диске или на дискете (в целях безопасности). Обычно связка личных ключей хранится в файле secring.skr, а связка открытых — в pubring.pkr. Эти файлы, как правило, располагаются в той же папке, в которой установлена PGP.

65. Найдите свои связки ключей по адресу: **C:/Program Files/Network Associates/PGP/PGP Keyrings**.

При работе с PGP может понадобиться исследовать или изменить атрибуты какого-либо ключа. Например, получив чей-либо открытый ключ, вы можете проверить его отпечаток или определить действительность на основе сертифицирующих его подписей. Может возникнуть необходимость изменить пароль доступа к своему личному ключу. Все подобные функции управления ключами доступны из окна PGPkeys (рис. 41).

Keys	Validity	Trust	Description	Creati...	Size	Key ID
Kirayeyv Nick <nicknicc@mail.ru>			DH/DSS public key	18.09.02	2048/1024	0x111936A7
Marina <Marinochka_n@mail.ru>			DH/DSS public key	18.09.02	2048/1024	0xE99790C9
Philip R. Zimmermann <prz@pgp.com>			DH/DSS public key	08.04.97	2048/1024	0xFAEBD5FC
Белая Оксана <Oksana@rambler.ru>			DH/DSS public key	18.09.02	2048/1024	0x247B433F
Ванцай Николай <wannik@mail.ru>			DH/DSS public key	18.09.02	2048/1024	0xE9E19332
Гейнц Александр Владимирович <alex_agro@mail.ru>			DH/DSS public key	18.09.02	2048/1024	0xE3A921F8
Есюкова Татьяна <ETanya@rambler.ru>			DH/DSS public key	18.09.02	2048/1024	0xD97E1AB2
Натали Милетто <natali@narod.ru>			DH/DSS key pair	24.07.03	2048/1024	0x76FA521C
Платошечкина Наталья <Platoshechkina@rambler.ru>			DH/DSS public key	18.09.02	2048/1024	0x60990B98
Ткаченко Алена <Alena_tkachenko>			DH/DSS public key	12.06.02	2048/1024	0x00C6AC0C
Чашевая Татьяна <tania@hotbox.ru>			DH/DSS public key	16.09.04	2048/1024	0x31301C13
Запольская Татьяна <Tatyana@rambler.ru>			DH/DSS public key	18.09.02	2048/1024	0xE62A807E
Зубарева Наталья <ZybarevaNV@mail.ru>			DH/DSS public key	18.09.02	2048/1024	0x416D581F
Фузеева Анна <fav@vipmail.ru>			DH/DSS public key	18.09.02	2048/1024	0xA29B4328
Мельникова Олеся <melnikova@rambler.ru>			DH/DSS public key	18.09.02	2048/1024	0x97BE3F37

Рис. 41. Окно PGPkeys

7.2. Окно PGPkeys

В окне PGPkeys (рис. 41) можно увидеть пары ключей созданными вами, а также все открытые ключи других пользователей, которые вы собрали. Значок  символизирует пару из личного и открытого ключа созданные вами, а значок  обозначает открытые ключи, полученные от других.

Большинство используемых в программе значков представлены в таблице 3.

Значки программы PGPkeys Таблица 3

	Желтый ключ и личико символизируют вашу пару ключей типа Diffie-Hellman/DSS. Пара состоит из открытого и личного ключей
	Одиночный желтый ключ символизируют личный ключ типа Diffie-Hellman/DSS
	Серый ключ и личико символизируют вашу пару ключей типа RSA. Пара состоит из открытого и личного ключей
	Одиночный серый ключ символизируют личный ключ типа RSA
	Когда ключ или пара ключей изображены серым цветом, это означает, что их использование временно запрещено
	Наличие картинки означает, что фотография пользователя соединена с открытым ключом
	Изображение ключа с красным крестиком означает, что ключ отозван
	Изображение ключа с часами означает, что срок действия ключа завершился. Срок действия ключа задается при генерации пары
	Конверт символизирует владельца ключа и список имен и адресов, связанных с ключом

	Серый круг означает недействительный ключ

Окончание табл. 3

	Зеленый круг означает действительный ключ
	Зеленый круг и личико, означает, что вы собственник ключа и полностью надежны
	Пустой прямоугольник означает недействительный ключ или ненадежного пользователя
	Наполовину заполненный прямоугольник означает отчасти действительный ключ или отчасти надежного пользователя
	Полосатый прямоугольник означает полностью действительный ключ или полностью надежного пользователя. Эти значения присваиваются только сгенерированным вами парам ключей
	Заполненный прямоугольник означает действительный ключ или надежного пользователя
	Перо обозначает подпись третьего лица, ручающегося за его подлинность

Щелкнув два раза на любом ключе, вы раскроете список, в котором будут отображены имена и адреса владельца, изображается конвертиком  . Щелкнув два раза на этом значке, вы увидите подписи всех тех, кто сертифицировал этот ключ. Эти подписи отображаются значком с изображением пера  (рис. 42).

Рис. 42. Окно PGPkeys

7.3. Атрибуты ключей

Вдоль верха главного окна PGPkeys расположены следующие метки, соответствующие атрибутам каждого ключа.

Keys (ключи) — символическое представление ключа, сопровождаемое именем и адресом его владельца.

Validity (действительность) — отображает степень уверенности в том, что ключ принадлежит номинальному владельцу. Действительность ключа вычисляется, исходя из того, кто сертифицировал ключ и насколько вы доверяете ручательствам этих лиц. Открытый ключ, который вы сертифицировали сами, обладает наибольшим уровнем действительности. Это основывается на допущении, что вы подпишите чей-либо ключ лишь тогда, когда будете полностью уверены в том, что он принадлежит владельцу. Действительность неподписанных лично вами ключей определяется исходя из уровня доверия, присвоенного вами третьим лицам, которые их сертифицировали. Если ключ несертифицирован никакими подписями, он рассматривается как недействительный.

Size (длина) — показывает количество бит, составляющих ключ. В общем, чем длиннее ключ, тем меньше вероятность того, что он будет скомпрометирован.

Trust (надежность) — указывает уровень доверия, которое вы присвоили владельцу ключа в смысле его способности быть посредником при сертификации ключей третьих лиц. Это значение используется, когда вы сами не можете определить действительность чьего-либо открытого ключа и решаете положиться на суждение третьих лиц, которые его сертифицировали. Когда вы генерируете свою пару ключей, они полностью считаются заслуживающими доверия, что символизируется полосками в полях действительности и надежности. Когда вы получаете открытый ключ, который был подписан кем-то, чей открытый ключ уже находится на вашей связке, подлинность определяется исходя из уровня надежности, который вы присвоили ключу сертифицировавшего новый ключ пользователя. Выделяют следующие уровни надежности: надежный (complete), отчасти надежный (marginal), ненадежный (untrusted).

Creation (создание) — показывает дату генерации ключа.

7.4. Свойства ключей

Кроме общих атрибутов, отображаемых в окне PGPkeys можно исследовать и изменять другие свойства ключей.

66. Просмотрите свойства ключа: выберите свой ключ, например, **Милетто Натали**, выберите **Keys | Properties.**

Key ID (идентификатор ключа) — уникальное число, связанное с ключом. Идентификатор нужен для того, чтобы различать разные ключи, носящие одинаковое имя пользователя и почтовый адрес**.**

Key Type (тип ключа) — тип ключа может быть RSA или Diffie-Hellman/DSS.

Key Size — длина ключа.

Created — дата, когда был создан ключ.

Expires — дата, когда истекает срок годности ключа. Владелец указывает эту дату при генерации новой пары и значение этого атрибута обычно “никогда” (never). Однако, некоторые ключи имеют определенный срок действия, если владелец захотел создать их для использования в течении определенного периода времени.

Модель доверия (trust model) — отображает действительность ключа, основываясь на сертифицирующих его подписях и уровне надежности, приданном теми, кто эти подписи наложил.

Отпечаток (fingerprint) — уникальный идентифицирующий номер, генерируемый при создании пары, и являющийся основным средством контроля подлинности ключа.

Разрешен (enabled) — эта опция указывает разрешено ли использование этого ключа. Временно запрещенный к использованию ключ отображается в окне PGPkeys серым цветом, и с его помощью невозможно выполнять какие-либо операции. Однако как только он вам снова понадобится, вы можете снова разрешить его использование.

Изменить пароль (change passphrase) — изменить пароль доступа к личному ключу. Обычно меняют пароль не реже одного раза в 6 месяцев.

7.5. Указание пары ключей по умолчанию

Если вы обладаете более чем одной парой ключей, вам может понадобиться явно обозначить одну пару, которая будет использоваться

по умолчанию. Текущая пара по умолчанию выделяется в окне жирным шрифтом.

67. Выберите ваш ключ, который вы хотите использовать по умолчанию, например, **Натали Милетто**, выберите **Keys,** выберите **Set As Default Key.**

7.6. Добавление нового имени или адреса

В некоторых случаях может понадобиться более чем одно имя или адрес, которые вы захотите связать с одной и той же парой ключей.

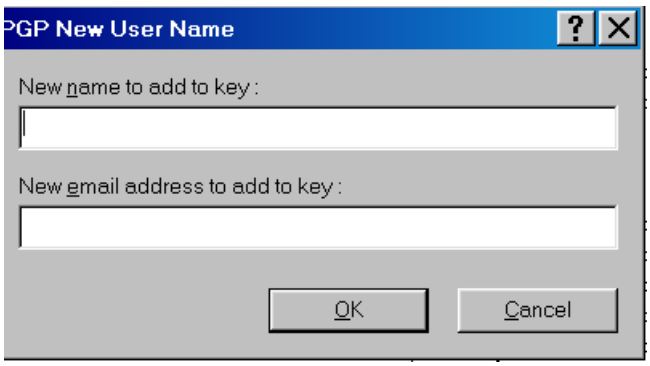

Рис. 43. Окно PGP New User Name

68. Введите новое имя: выберите свой ключ, например, **Натали Милетто**, выберите **Keys,** выберите **Add Name**, в поле **New name to add to key** введите новое имя, например, **Наташа**, в поле **New email to add to key** введите Email, **natali@yandex.ru**, нажмите **ОК** (рис. 43), в поле **Enter passphrase…** введите ваш пароль для тайного ключа, например, **ЯлюблюРозовыеОблака!,** нажмите **ОК**.

7.7. Проверка отпечатка ключа

Часто трудно быть уверенным, что ключ принадлежит определенному лицу, если вы не получили этот ключ непосредственно от него на дискете. Тем более обмен ключами с помощью дискеты не подходит, если ваш товарищ находится от вас на расстоянии в тысячи километров. В этом случае удобно использовать отпечаток ключа. Для проверки ключа наиболее надежно позвонить владельцу и попросить прочитать отпечаток по телефону. Маловероятно, что звонок перехватят и сумеют сымитировать голос вашего собеседника. Также вы можете сравнить отпечаток вашей копии чьего-либо ключа с отпечатком копии, хранящейся на сервере открытых ключей.

69. Просмотрите отпечаток ключа: выберите ключ своего товарища, например, **Фузеева Анна**, выберите **Keys | Properties**, **Finger-**

print, где 7FC0 5BFB 5E97 0496 29CC 1D58 7D03 2C9B A29B 4328 — уникальный идентификационный номер, создаваемый при создании пары ключей и являющийся средством контроля подлинности ключа.

7.8. Сертификация чужого открытого ключа

Когда вы создавали свою пару ключей, она автоматически подписывается с помощью вашего личного ключа. Точно также после того как вы убедились, что полученный вами открытый ключ действительно принадлежит его владельцу, вы можете подписать (сертифицировать) этот ключ, указывая, что вы уверены в его действительности.

70. Подпишите открытый ключ вашего товарища: см. 49.

7.9. Указание уровня доверия

Кроме сертификации принадлежности ключа владельцу, вы можете присвоить его владельцу определенный уровень доверия, указывающий, насколько вы доверяете ему выступать в качестве посредника, ручающегося за целостность ключей, которые вы можете получить в будущем. Это значит, что если вы когда-нибудь получите от кого-либо ключ, подписанный лицом, которого вы обозначили как заслуживающий доверия, ключ может рассматриваться как действительный, даже если вы не проверяли его подлинность сами.

71. Выберите ключ своего товарища, например, **Ткаченко Алена**, выберите **Keys**, выберите **Properties**, ползунком выберите **отчасти надежный** уровень (рис. 44), нажмите **ОК**.

Рис. 44. Область Trust Model

7.10. Запрет и разрешение использования ключей

Иногда может понадобиться возможность временного запрета использования ключа.

72. Запретите ключ: выберите ключ своего товарища, например, **Ткаченко Алена**, выберите **Keys**, выберите **Properties**, выберите **Disable**, нажмите **ОК**.

73. Разрешите ключ: выберите ключ своего товарища, например, **Ткаченко Алена**, выберите **Keys**, выберите **Properties**, выберите **Enable**, нажмите **ОК**.

7.11. Удаление ключа

Вам может понадобиться удалить ключ, сертифицирующую его подпись или идентификатор пользователя.

74. Удалите подпись ключа: выберите свой ключ, например, **Натали Милетто, M2**, выберите идентификатор (User ID) **Наташа, M2**, выберите подпись **Наташа, МП**, выберите **Delete**, выберите **Да**.

75. Удалите идентификатор пользователя: выберите свой ключ, например, **Натали Милетто, M2**, выберите идентификатор (User ID) **Наташа, МП**, выберите **Delete**, выберите **Да**.

7.12. Изменение пароля доступа

Необходимо периодически менять пароль доступа к своему личному ключу.

76. Измените пароль: выберите ключ, например, **Натали Милетто, МП**, выберите **Keys Properties**, выберите **Change Passphrase**, введите пароль **ЯлюблюРозовыеОблака!** (рис. 45)**,** нажмите **ОК**,

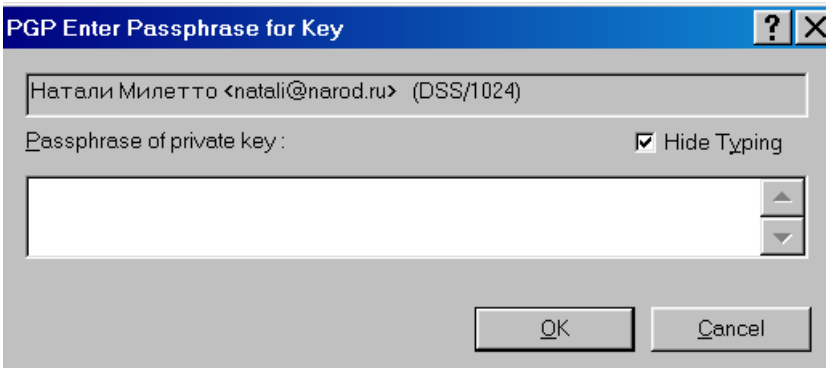

Рис. 45. Окно PGP Enter Passphrase for Key

введите новый пароль **ЯлюблюЖелтыеОблака!** и его подтверждение (рис. 46), нажмите **ОК**.

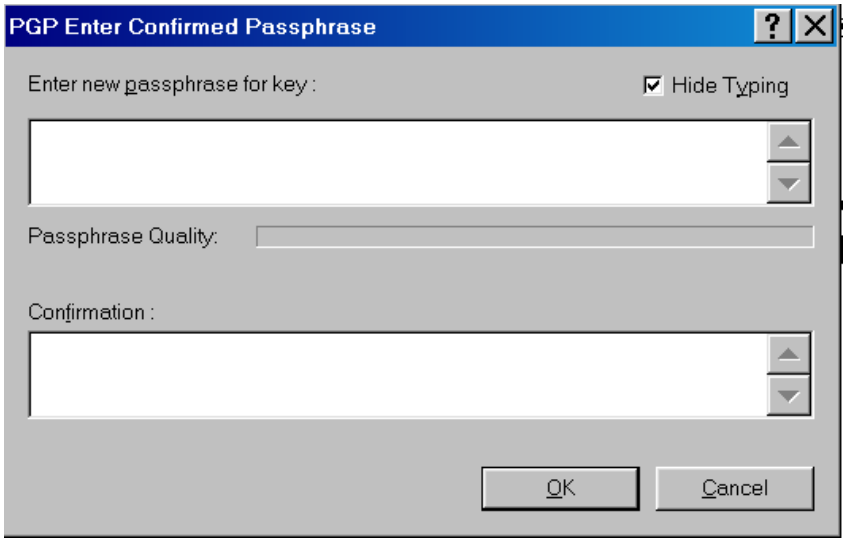

Рис. 46. Окно PGP Enter Confirmed Passphrase

7.13. Добавление фотографии

77. Добавьте фотографию: выберите свой ключ, например, **Натали Милетто**, выберите **Keys | Add | Photo**, выберите **Select File**, выберите файл с изображением в форма **JPG** или **BMP**, нажмите **OK**, введите ваш пароль, например, **ЯлюблюЖелтыеОблака!** нажмите **ОК**.

7.14. Окончательное удаление файлов

Потенциальная проблема безопасности связана со способом, которым большинство операционных систем удаляет файлы [1]. Когда вы шифруете файл и затем удаляете файл с исходным открытым текстом, система не стирает данные физически. Она просто помечает соответствующие блоки на диске как свободные, допуская тем самым повторное использование этого пространства. Это похоже на то, как если бы ненужные секретные документы выбрасывались в мусорную корзину вместо того, чтобы отправить их в специальное устройство для уничтожения бумаг. Эти блоки диска все еще сохраняют исходные секретные данные, которые вы хотели стереть, и лишь со временем будут заняты новыми данными. Если вор прочитает эти блоки данных вскоре после того, как они помечены как свободные, он сможет восстановить ваш исходный открытый текст.

Это может произойти и случайно: если из-за какого-нибудь сбоя будут уничтожены другие файлы, для их восстановления запустят программу восстановления, а она восстановит также и некоторые из ранее стертых файлов. Может случиться так, что среди последних окажутся и ваши конфиденциальные файлы, которые вы намеревались уничтожить без следа, но они могут попасться на глаза тому, кто восстанавливает поврежденный диск.

Даже когда вы создаете исходное сообщение с использованием текстового редактора, программа может оставить множество промежуточных временных файлов просто потому, что она так работает. Эти временные файлы обычно удаляются редактором при его закрытии, но фрагменты вашего секретного текста остаются где-то на диске.

Единственный способ предотвратить восстановление открытого текста — это каким-либо образом обеспечить перезапись места, занимаемого удаленными файлами. Это можно осуществить, используя любую утилиту, которая способна перезаписать все неиспользован-

ные блоки на диске. В PGP для этого есть функция **Wipe** для окончательного удаления файлов. А функция **Freespace Wipe** предназначена для удаления всех временных файлов на жестком диске.

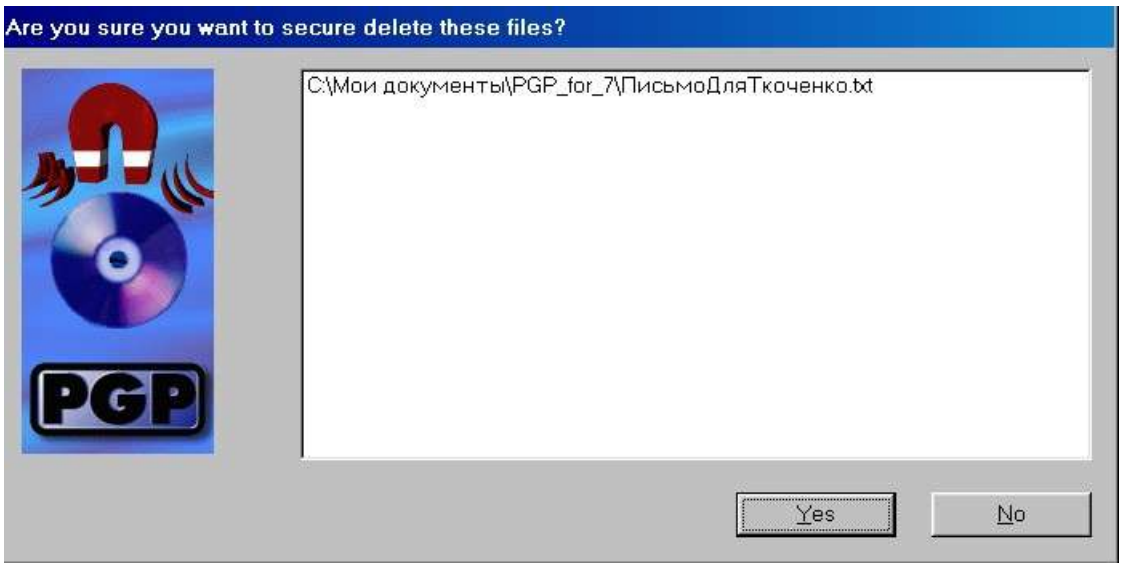

Рис. 47. Окно Wipe

78. Удалите файл по настоящему: **Пуск | Программы | Проводник**, выберите созданный вами файл, например, **ПисьмоДляТкаченко**, **МП**, выберите **PGP | Wipe**, нажмите **Yes** (рис. 47).

8-й день. Шифрование дисков

Все было просто: пол дубовый,
Два шкафа, стол, диван пуховый,
Нигде ни пятнышка чернил.
Онегин шкафы отворил:
В одном нашел тетрадь расхода,
В другом наливок целый строй,
Кувшины с яблочной водой
И календарь осьмого года…

А.С. Пушкин. Евгений Онегин

8.1. PGP Disk

Большинство руководителей разъезжают по миру с компьютером в чемодане. Естественно, на таком компьютере есть секретные данные. Представим, что случилась неприятность — компьютер украли. Практически гарантированно, что воры получат информацию с жесткого диска. Дело в том, что популярные файловые системы, например, FAT, FAT32, NTFS, ext2, ufs, позволяют прочитать данные при физическом доступе к носителю. То есть если у вас в руках оказался жесткий диск — то данные с него можно прочитать. Поэтому, серверы располагают обычно в недоступных местах — так как современные файловые системы обеспечивают защиту при сетевом доступе, но не при физическом [13].

Поэтому одним из важных компонентов криптографической системы PGP является модуль PGP Disk для шифрования данных на жестких дисках.

Схема работы модуля состоит в следующем. На обычном диске создается файл-криптоконтейнер (в любом каталоге с любым именем и расширением), который при штатной работе отображается в логический диск. При создании вы указываете емкость диска, алгоритм защиты и букву, которой будет назван диск после подключения.

Вся информация в файле-контейнере шифрованная. То есть, получив этот файл и не зная пароля, его практически невозможно расшифровать.

Хотя это всего лишь один файл (например, natali.pgd), он действует подобно жесткому диску в том отношении, что он выполняет функцию хранения файлов и программ. При этом файл-контейнер можно свободно переименовывать, копировать и вообще проводить с

ним любые операции (только если в данный момент диск не подключен).

Для того, чтобы использовать программы и файлы, находящиеся на таком диске, вы его устанавливаете командой **Mount**, после чего его можно использовать также, как любой другой диск. Теперь нет необходимости шифровать большое количество файлов, в которых находится конфиденциальная информация. Можно переместить все конфиденциальные файлы на такой диск и таким образом избежать необходимости каждый раз расшифровывать какой-либо файл при его открытии.

После того, как вы отключите этот диск командой **Unmount**, он станет недоступным для третьих лиц и для того, чтобы открыть его, необходимо ввести парольную фразу, которая известна только вам. Но даже разблокированный диск защищен от несанкционированного доступа. Если ваш компьютер зависнет во время использования диска, то его содержание будет зашифровано.

8.2. Создание нового PGP диска

79. Создайте новый PGP диск: выберите **замочек**, **МП**, выберите **PGPdisk**, после чего появится окно программы (рис. 48) со следующими командами:

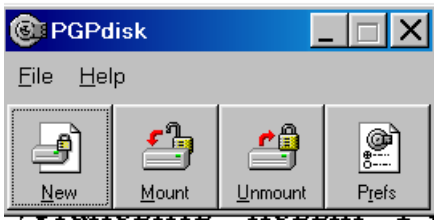

Рис. 48. Окно PGPdisk

New — создать новый PGP диск;

Mount — установить созданный диск;

Unmount — закрыть диск, который был ранее установлен;

Prefs – опции настройки.

80. Выберите **New**, после чего на экране появится мастер создания PGP диска (рис. 49), выберите **Далее**.

81. В окне **New PGPdisk** (рис. 50) выберите место расположения диска: в поле **Папка** выберите **Мои документы**, в поле **Имя файла** введите **Natali**, выберите **Сохранить**.

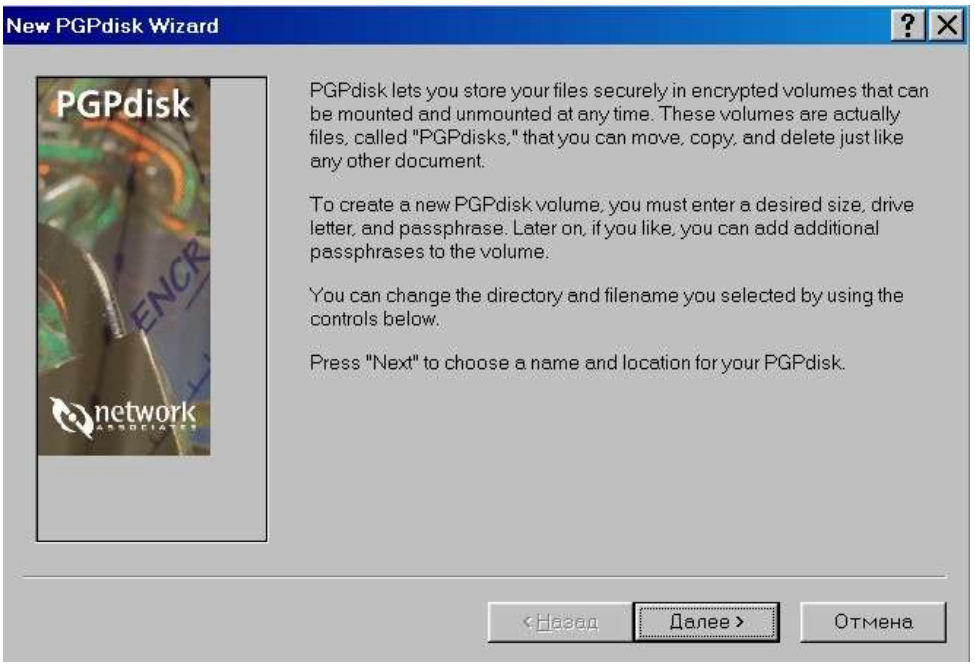

Рис. 49. Окно New PGPdisk Wizard

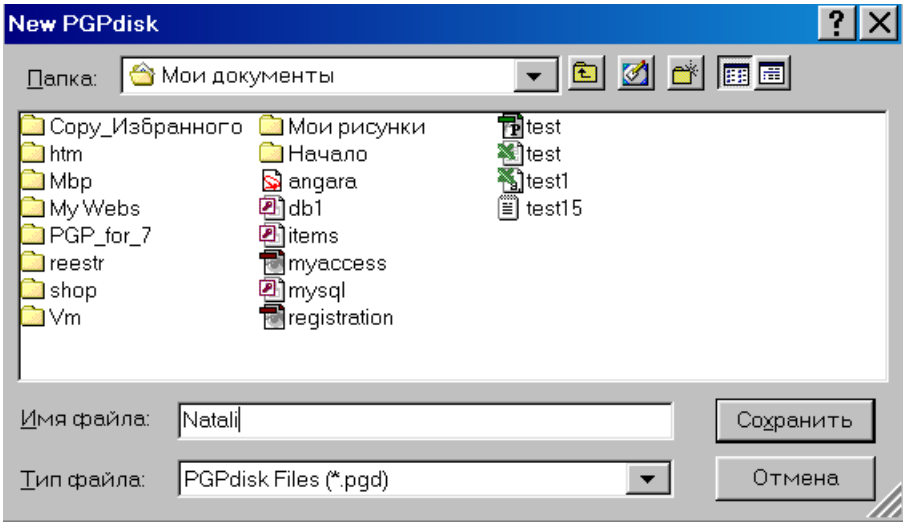

Рис. 50. Окно New PGPdisk

82. В области **PGPdisk Size** выберите цифру, обозначающую размер PGP диска, например, **100**, и не забудьте там же выбрать размерность в килобайтах **KB** (рис. 51).

83. В области **PGPdisk Drive Letter** выберите букву, которую вы присвоите новому диску (рис. 51), например, **E**, нажмите на **Далее.**

Рис. 51. Окно PGPdisk Size

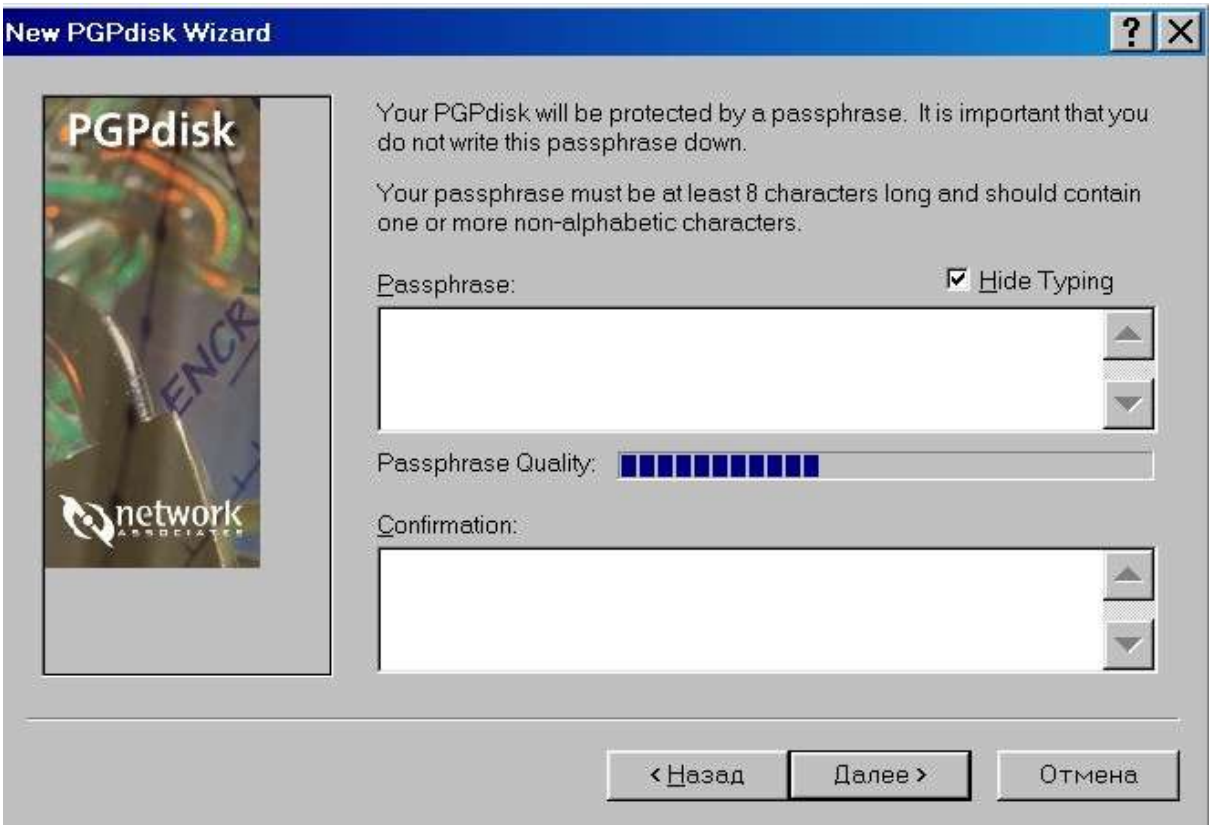

Рис. 52. Окно PGPdisk Passphrase

84. В поле **Passphrase** введите парольную фразу, например, **ЯлюблюСинииеОблака!**, введите тот же пароль **ЯлюблюСинииеОблака!** в поле **Confirmation**, выберите **Далее** (рис. 52)**.** Подвигайте мышку или нажимайте на кнопки на клавиатуре для того, чтобы программа сгенерировала данные для создания ключа. Как только столбик остановится на 100% нажмите на **Далее.**

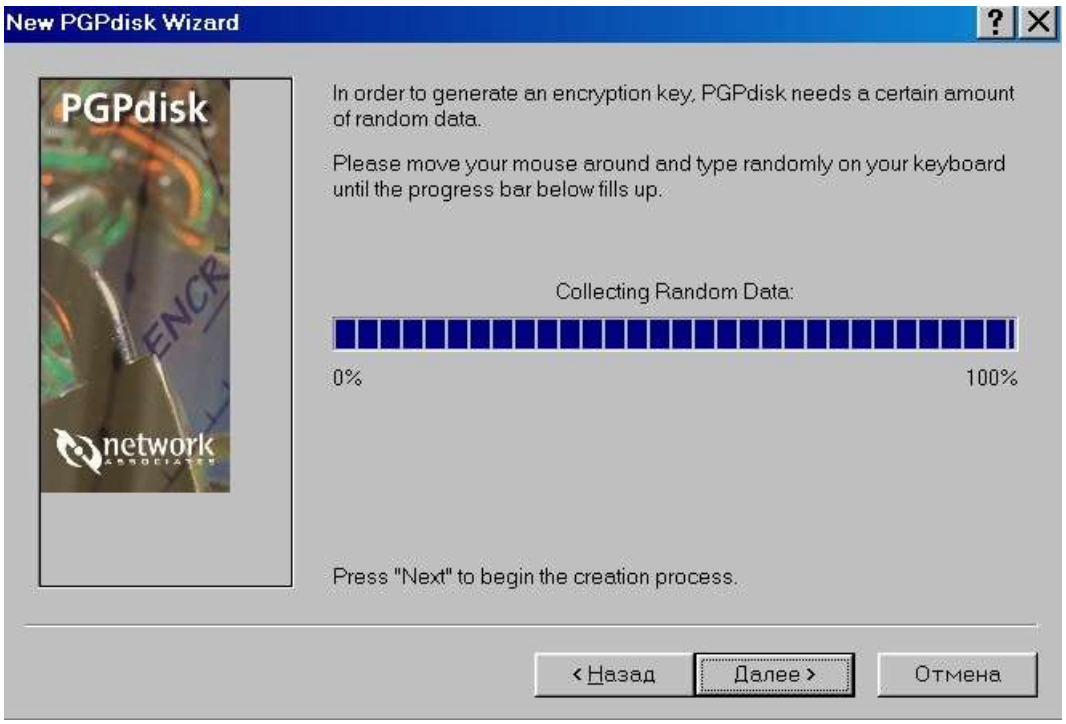

Рис. 53. Окно окончания генерации ключа

85. Нажмите на **Далее** (рис. 53), чтобы начать процесс создания диска.

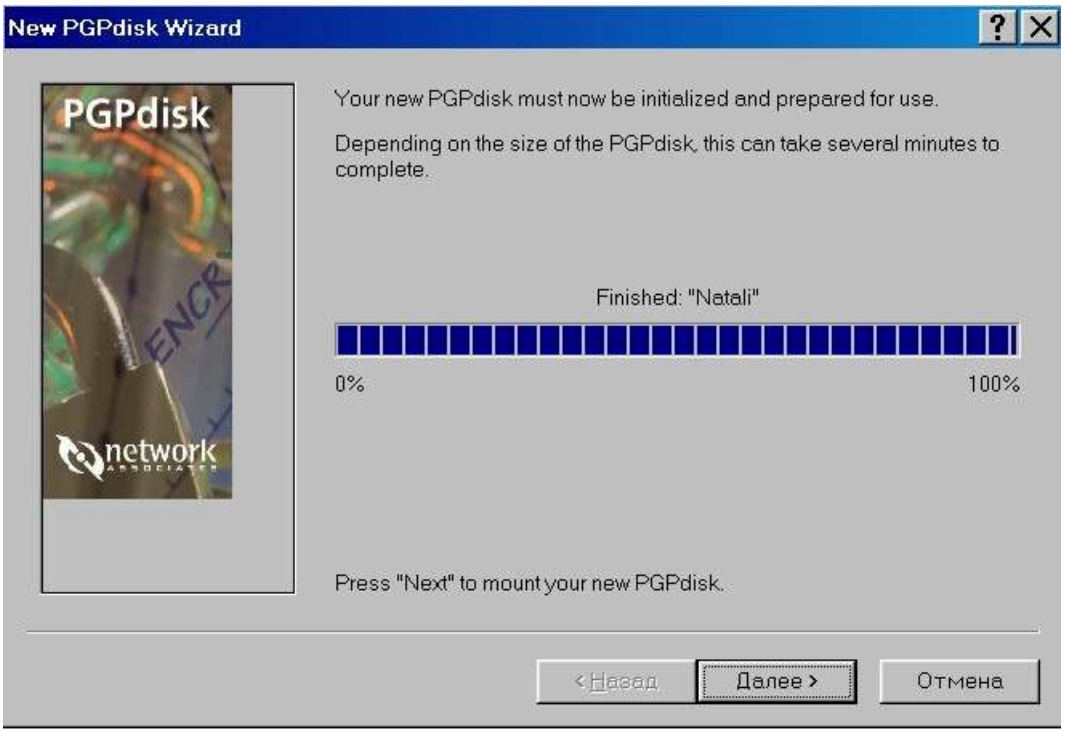

Рис. 54. Окно начала установки диска

86. Нажмите на **Далее** (рис. 54), чтобы установить PGP диск.

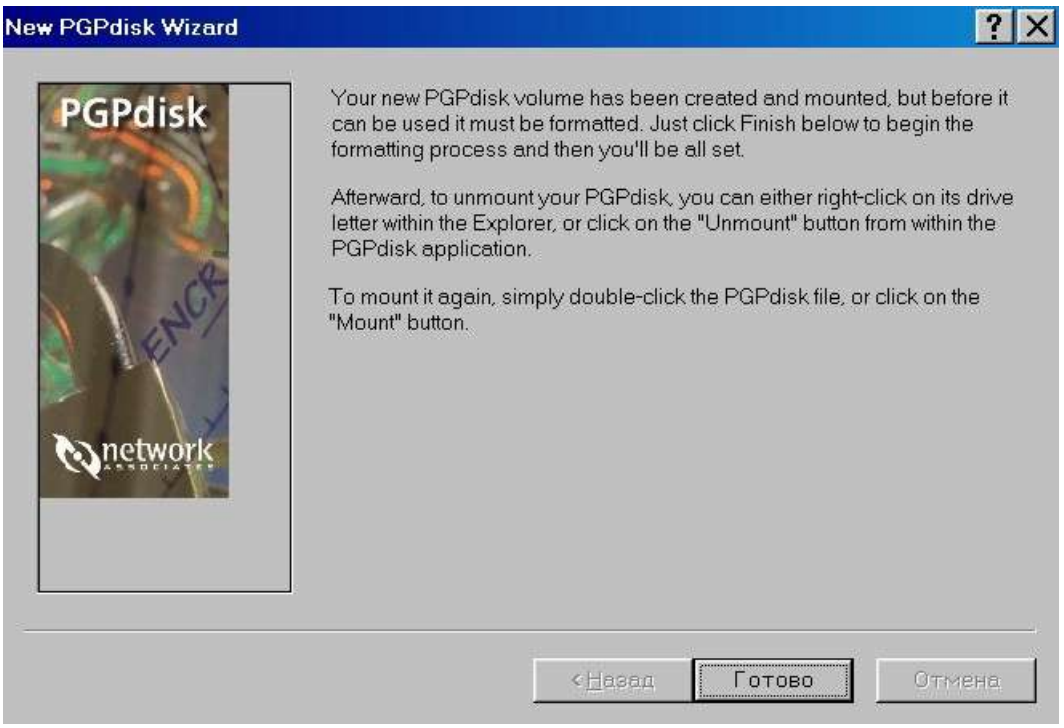

Рис. 55. Окна окончания установки диска

87. Нажмите на **Готово** (рис. 55).

88. Выберите способ форматирования **Полное**, в поле **Метка** введите название нового диска **Natali,** выберите **Начать**, начнется форматирование, после окончания выберите **Закрыть**.

89. Нажмите на кнопку **Закрыть** на окне форматирования.

Как только новый диск будет создан, программа PGP автоматически его установит с тем, чтобы вы могли начать его использовать.

90. Просмотрите новый диск: **Пуск | Программы | Проводник**, выберите диск **E**, он пустой.

После того, как вы закончили работу с конфиденциальной информацией, необходимо отключить диск. После отключения диска его содержимое будет зашифровано в виде зашифрованного файла.

91. Закройте PGP диск: выберите **E: | МП,** выберите **PGPdisk | Unmount PGPdisk.**

8.3. Открытие и закрытие PGP диска

Для открытия PGP диска надо дважды щелкнуть по нему мышкой и ввести парольную фразу в появившееся окно программы. Вы сможете убедиться в том, что PGP диск открылся, зайдя в папку «Мой компьютер» и увидев, что рядом с диском C появился диск E. Также можно открыть PGP диск используя программу PGPtray.

92. Откройте PGP диск: выберите **замочек**, **МП**, выберите **PGPdisk**, должно появится окно программы **PGPdisk**, нажмите **Mount**, выберите **natali.pgd**, выберите **Открыть**, введите парольную фразу **ЯлюблюСиниеОблака!**, нажмите **ОК** (рис. 56) .

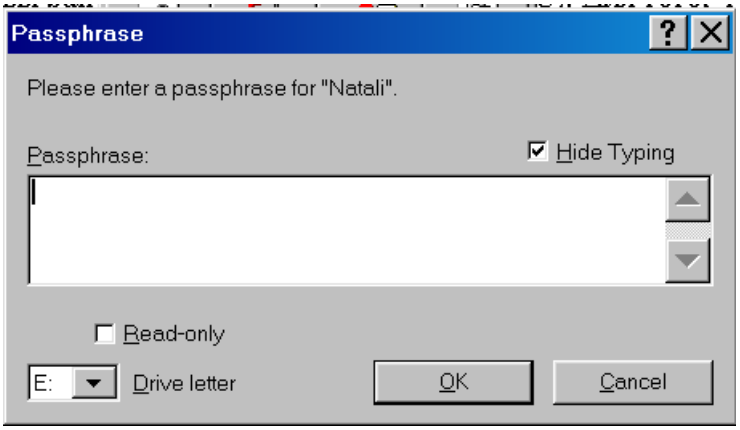

Рис.56. Окно Passphrase

На диске PGP можно создавать файлы, каталоги, перемещать файлы или каталоги, либо удалять, т.е. можно делать те же самые операции, что и на обычном диске.

93. Скопируйте на PGP диск парочку файлов.

94. Закройте все программы и файлы, имеющиеся на диске PGP, т.к. невозможно закрыть диск, если файлы на этом диске до сих пор еще открыты.

95. Закройте PGP диск: на панели задач выберите **PGPdisk**, нажмите **Unmount**, выберите диск **Natali (E),** нажмите **Unmount**.

Как только диск будет закрыт, то он исчезнет из окна Проводника и превратится в зашифрованный файл **natali.pgd**.

8.4. Настройки

Еще один важный момент, на который необходимо обратить внимание, это настройки программы, которые позволяют автоматически закрыть диск в случае не обращения к диску в течение какого-либо периода времени.

96. Выполните настройки: на панели задач выберите **PGPdisk**, нажмите **Prefs** и в появившемся меню под названием **Auto Unmount** (автоматическое закрытие) выберите флажком **auto unmount after _ minutes of inactivity** (автоматически закрыть после минут бездействия), укажите количество минут **15**, выберите флажком **auto unmount on computer sleep** (автоматически закрыть при переходе компьютера в спящее состояние), нажмите **ОК**.

8.5. Горячие слова*

* В разделы использованы материалы из [16].

AES (Advanced Encryption Standard). Расширенный стандарт шифрования — стандарт, одобренный Американским национальным институтом стандартизации (NIST) для использования в ближайшие 20-30 лет.

Algorithm encryption. Алгоритм шифрования — набор математических правил, используемый для шифрования и расшифровки.

Algorithm hash. Хэш-алгоритм — набор математических правил, используемый для создания дайджеста сообщения и для генерации ключа/подписи.

Anonymity. Анонимность — сокрытие происхождения или авторства материала (сообщения).

ANSI (American National Standards Institute). Американский институт стандартов — один из ведущих мировых центров в области разработки стандартов. Его новое название — NIST — National Institute of Standards and Technology. Разрабатываемые им стандарты используются в качестве базы для создания международных стандартов ISO/IEC.

ASCII-armored text. Защищенный текст ASCII — двоичная информация, закодированная только с использованием стандартных печатаемых символов, входящих в набор ASCII (American Standard Code for Information Interchange). В таком виде информация пригодна для передачи по любым сетевым каналам. PGP использует для шифровки/расшифровки ASCII-текстов формат radix-64. В таком виде информация пригодна для передачи по любым сетевым каналам. PGP придает по умолчанию именам файлов содержащих ASCII-текст расширение asc.

Asymmetric keys. Ассиметричные ключи — отдельные, но взаимосвязанные ключи; пара ключей включает один открытый ключ и один личный ключ. То, что зашифровано одним ключом, может быть расшифровано другим ключом и только им.

Authentication. Аутентификация — проверка подлинности, определение происхождения документа путем проверки цифровой подписи автора или открытого ключа по уникальному отпечатку.

Authorization certificate. Сертификат авторизации —электронный документ, подтверждающий право доступа к информации, какие-либо иные права или личность предъявителя.

AH (Authentication Header). Аутентификационный заголовок — протокол обеспечения безопасности, содержит средства проверки подлинности. AH встраивается в данные и может использоваться как сам по себе, так и в сочетании с Encryption Service Payload (ESP).

Blind signature. «Слепая подпись» — подписывание документов без просмотра их содержимого.

Block cipher. Блок-шифр — симметричный шифр, состоящий из блоков открытого текста и зашифрованного текста. Обычно блок имеет размер 64 бит.

Backdoor. «Черный ход» — слабое место в шифровальной системе, случайного или запланированного происхождения. Через «черный ход» информированный человек может легко преодолеть защиту. Когда механизм действия шифра держится в секрете, наблюдатели обычно подозревают наличие «черного хода».

CA (Certificate Authority). Сертифицирующий орган — доверенное «третье лицо», которое выдает сертификаты с перечислением определенных свойств и присваивает эти сертификаты конкретному лицу/организации или его/ее открытому ключу.

CAPI (Crypto API) — криптографический прикладной программный интерфейс Microsoft для разработчиков программ для операционных систем Windows.

CAST — 64-битовый блок-шифр, разработанный в Канаде Адамсом и Таваресом.

Certificate (digital certificate). Сертификат (цифровой сертификат) — электронный документ, которым доверенное третье лицо снабжает открытый ключ пользователя. Сертификат подтверждает, что ключ действует и реально принадлежит этому пользователю.

Certification. Сертификация — выдача информации доверенным третьим лицом (организацией).

Certify. Сертифицировать — подписывать чей-либо открытый ключ.

Certifying authority. Уполномоченный сертификатор — доверенное третье лицо (или группа лиц), которому даны полномочия для сертификации ключей и внесения их в общую базу данных.

Cipher text. Зашифрованный текст, шифр — обычный текст, преобразованный в формат, который обеспечивает секретность, посредством какого-либо шифровального алгоритма. Чтобы раскрыть шифр, необходим ключ.

Clear text. Чистый текст — текст, который может быть легко прочитан человеком или машиной (говорят также plain text).

Clear-signed message — сообщение, которое не было зашифровано, но содержит цифровую подпись.

Corporate signing key. Корпоративный ключ подписи — ключ, создаваемый службой безопасности компании и являющийся ключом «по умолчанию» для сертификации других ключей от лица компании.

Conventional encryption. Традиционное шифрование — шифрование, основанное на обычном пароле (а не на открытом ключе). Файл шифруется с помощью сессионного ключа, для активации которого необходимо ввести пароль.

Cryptanalysis. Криптоанализ — умение (наука) получать открытый текст из шифра без знания ключа, которым был зашифрован открытый текст.

Cryptography. Криптография — умение (наука) преобразовывать в секретный формат сообщения конфиденциального характера.

Cryptosystem. Криптосистема — система криптографических алгоритмов, доступных открытых текстов, шифров и шифровальных ключей.

Data integrity. Целостность данных — обеспечение защиты данных от несанкционированного изменения.

Decryption. Расшифровка — преобразование зашифрованной информации в читаемый вид. Для расшифровки используется личный ключ получателя.

DES (Data Encryption Standard). «Стандарт шифрования данных» — 64-битный блоковый шифровальный симметричный алгоритм, известный также под названием DEA и DEA-1. Разработанный в 1976 году под названием FIPS 46 был первым в мире открытым официальным стандартом шифрования.

Dictionary attack. «Словарная атака» — попытка определить пароль «в лоб» путем перебора наиболее вероятных комбинаций слов.

Diffie-Hellman algorithm. Алгоритм Диффи-Хеллмана — первый известный алгоритм с использованием открытого ключа. Предложен в 1976 г., использует дискретные логарифмы в конечных полях.

Digital cash. Цифровые деньги — «электронная наличность», которая хранится и передается с помощью различных сложных протоколов.

Direct trust. «Прямое доверие» — установка доверительных отношений без посредников.

Digital signature. Цифровая подпись.

DSA (Digital Signature Algorithm) — алгоритм цифровой подписи, с использованием открытого ключа. Предложен NIST для использования в стандарте DSS.

DSS (Digital Signature Standard) — стандарт, предложенный NIST (известен также как FIPS) для цифровых подписей.

ECC (Elliptic Curve Cryptosystem) — криптосистема эллиптических кривых. Основа алгоритмов открытых ключей с использованием математических кривых в конечных полях или с использованием больших простых чисел.

EES (Escrowed Encryption Standard) — стандарт шифрования, предложенный правительством США для обеспечения доступа к секретным ключам.

Elgamal scheme — схема, используемая как для цифровых подписей, так и для шифрования. Основана на дискретных логарифмах в конечных полях, может использоваться в сочетании с DSA.

Encryption. Шифрование — преобразование информации в формат, непонятный никому, кроме адресата, который должен расшифровать сообщение для того, чтобы его прочитать.

Fingerprint. Отпечаток — строка из чисел и букв, однозначно идентифицирующая открытый ключ. Является основным средством определения принадлежности ключа.

FIPS (Federal Information Processing Standard) — федеральный стандарт обработки информации. Правительственный стандарт США, определяемый NIST.

Firewall. Брандмауэр (межсетевой экран) — комплекс аппаратных и программных средств, защищающих компьютерную сеть от определенных атак извне.

Hash function. Хэш-функция — однонаправленная функция, которая при аргументе произвольной длины возвращает значение постоянной длины.

Hierarchical trust. Иерархия доверенных лиц — совокупность лиц (организаций), где доверенность распределяется между ее членами. Обычно используется для сертификации по стандарту ANSI X.509.

HTTP (HyperText Transfer Protocol). Протокол передачи гипертекста — используется для передачи документов с одного Интернет-сервера на другой или с сервера клиенту.

IDEA (International Data Encryption Standard). Международный стандарт шифрования данных — 64-битовый блоковый симметричный алгоритм шифрования с использованием 128-битовых ключей, основанных на смешанных операциях в различных алгебраических группах. Считается одним из наиболее стойких алгоритмов.

IKE (Internet Key Exchange). **Обмен ключами в Интернете** — обеспечение безопасности обмена ключами в Интернете. IKE рассматривается как один из вариантов реализации IPSec.

Implicit trust. Полное доверие — характеристика пар ключей, находящихся на компьютере. Если на вашем компьютере для открытого ключа находится парный ему личный, PGP считает, что вы — хозяин обоих ключей, а значит, безоговорочно себе доверяете.

Integrity. Целостность данных — гарантия, что данные не подвергались несанкционированному изменению во время хранения или передачи.

Introducer. Посредник — лицо или организация, которое обладает полномочиями судить об аутентичности ключей. Вы назначаете посредников, подписывая их открытые ключи.

IPSec — система обеспечения безопасности в семействе протоколов TCP/IP.

IEC (International Electrotechnical Commission). Международная комиссия по электротехнике — одна из ведущих международных организаций в области разработки стандартов. Стандарты разрабатываются совместно с ISO и обозначаются ISO/IEC.

ISO 9594-8: 1988 — «Взаимосвязь открытых систем. Справочник. Часть 8: Основы аутентификации». Международный стандарт.

ISO 9796: 1991 — «ИТ. Средства безопасности. Схема цифровой подписи с возможностью восстановления сообщения». Международный стандарт.

ISO 9797: 1989 — «ИТ. Криптографические методы защиты. Механизм удостоверения целостности данных, использующих функцию криптографической контрольной суммы на базе блочного алгоритма шифрования». Международный стандарт.

Key. Ключ — цифровой код, используемый для шифрования, подписи, расшифровки сообщений, а также проверки подписи. Ключи составляют пары и хранятся в связках.

Key escrow/recovery — практика передачи пользователями копий своих секретных ключей третьей стороне. Последняя, таким образом, получает доступ к содержанию зашифрованной переписки.

Key exchange. Обмен ключами — схема, в которой два и более узла обмениваются секретными ключами, используя незащищенный канал.

Key fingerprint. Отпечаток ключа — строка чисел или букв, однозначно аутентифицирующая открытый ключ. Вы можете, например, позвонить по телефону владельцу открытого ключа и попросить продиктовать отпечаток ключа с тем, чтобы вы могли сравнить его с отпечатком своей копии. Если отпечатки не совпадают, это значит, что ваша копия — подделка.

Key ID. Идентификатор ключа — читаемая строка, которая однозначно идентифицирует пару ключей. Две разные пары ключей могут иметь одинаковые идентификаторы пользователя, но идентификаторы ключа у них будут разные.

Key length. Длина ключа — число битов, определяющее размер ключа: чем длиннее ключ, тем он надежнее.

Key management. Управление ключами — процесс безопасной генерации, хранения и распространения криптографических ключей.

Key pair. Пара ключей — открытый ключ и дополняющий его личный ключ. В системах, основанных на алгоритмах открытых ключей (таких, как PGP), каждый пользователь имеет, по крайней мере, одну пару ключей.

Keyring. Связка ключей — у каждого пользователя две связки (набора) ключей: связка открытых ключей и связка личных ключей

Key splitting. Разделение ключей — личный ключ делится на части, которые затем распределяются между несколькими людьми. Определенное число владельцев частей ключа, собравшихся вместе, могут восстановить ключ и использовать его.

Message digest. Дайджест сообщения — компактный «дистиллят» сообщения или контрольная сумма файла. Дайджест зависит от содержания сообщения: если хоть немного изменить содержание, изменится и дайджест.

Meta-introducer — посредник, являющийся доверенным лицом другого посредника.

MD5 — один из лучших алгоритмов одностороннего хэширования, разработан Ривестом (Rivest).

MIME (Multipurpose Internet Mail Extensions) — свободно распространяемый набор спецификаций, который позволяет обеспечить текстом в различных языковых кодировках, а также использовать мультимедиа в сообщениях электронной почты.

Non-repudiation. Предотвращение разрыва — предотвращает отказ от предыдущей операции или разрыв связи.

Passphrase. Фраза-пароль — легко запоминаемая фраза, более надежный пароль, чем просто слово.

Password. Слово-пароль — последовательность знаков или слово, которое требуется для аутентификации.

PGP/MIME — стандарт IETF (RFC 2015), который обеспечивает секретность и аутентификацию с использованием стандарта MIME (RFC1847). Реализован в PGP версии 5.0 и выше.

PFS (Perfect Forward Secrecy) — гарантия того, что (в случае асимметричного шифрования) временный ключ, вычисленный из набора открытых и секретных ключей, не будет скомпрометирован и в том случае, если какой-либо из секретных ключей будет скомпрометирован.

PKCS (Public Key Crypto Standards). Стандарты открытых ключей — разработаны консорциумом организаций (Apple, DEC, Lotus, Microsoft, MIT, RSA и Sun), бывают как зависимыми от алгоритма

шифрования, так и независимыми. Отдельные спецификации и протоколы контролируются RSA Data Security Inc.

PKI (Public Key Infrastructure). Инфраструктура открытых ключей — распространенная система сертификации, при которой, получая чей-то ключ, вы можете быть в определенной степени уверены, что этот ключ действительно принадлежит его хозяину и не является подделкой.

Plaintext. Открытый текст — обычный читаемый (незашифрованный) текст.

Private key. Личный ключ — один из пары ключей (другой ключ — открытый). Используется для подписывания и расшифровки данных. Личный ключ следует хранить в тайне и не допускать к нему посторонних.

Private keyring. Связка личных ключей — личные ключи, принадлежащие владельцу связки.

Public key. Открытый ключ — один из пары ключей (другой ключ — секретный). Используется для шифрования информации и проверки подписей. Открытый ключ можно свободно распространять. Обладание чьим-либо открытым ключом не дает никакой пользы злоумышленнику, желающему вскрыть шифр.

Public keyring. Связка открытых ключей — ваша связка включает и ваш собственный открытый ключ.

Public-key cryptography. Криптография с открытым ключом — криптографическая система, в которой используются открытый и секретный ключи, а канал связи может быть незащищенным.

Random number. Случайное число — генератор случайных (псевдослучайных) чисел является составной частью многих криптосистем. С его помощью можно создавать уникальные ключи, которые невозможно вычислить заранее. Наиболее совершенные генераторы случайных чисел основаны на данных, полученных из аналоговых источников, и, как правило, требуют использования специального оборудования.

Revocation retraction of certification or authorization. Отмена сертификации или авторизации.

RFC (Request for Comment). «Требуется комментарий» — документ IETF, содержащий обзор или представление Интернет-стан-

дартов. Каждый RFC имеет свой номер, который можно использовать при поиске или ссылках (http://www.ietf.org).

RSA — краткое название компании RSA Data Security, Inc.; также название шифровального алгоритма – по первым буквам имен его изобретателей (Ривест, Шамир, Адельман). Алгоритм RSA используется в системах шифрования с открытым ключом. В основе алгоритма лежит факт сложности определения больших простых чисел по их произведению.

Secure channel. Безопасный канал — передача информации от одного лица другому, при которой третье лицо не может изменять порядок сообщений, удалять, добавлять или читать информацию.

Self-signed key. Ключ, подписанный его автором — открытый ключ, подписанный при помощи парного к нему секретного ключа.

Session key. Временный (сессионный) ключ — используется для шифрования в симметричных алгоритмах. Для шифрования каждого сеанса связи применяется новый ключ.

Sign — подписывать.

Signature. Подпись — цифровой код, созданный с помощью секретного ключа. Подпись позволяет аутентифицировать информацию с помощью процедуры проверки подписи. Когда вы подписываете сообщение или файл, PGP использует ваш личный ключ, для создания цифрового кода, однозначно связанного с текстом сообщения и закрытым ключом. После чего вашу подпись можно проверить с помощью вашего открытого ключа.

S/MIME (Secure Multipurpose Mail Extension) — рекомендуемый стандарт, разработанный Deming software и RSA Data Security для расшифровки и/или подтверждения подлинности данных MIME. S/MIME определяет формат данных MIME, алгоритмы, с помощью которых устанавливается взаимодействие (RSA, RC2, SHA-1), и наличие дополнительных вещей, таких как сертификаты ANSI X.509 и передача информации через Интернет.

SSL (Secure Socket Layer). Защищенный транспортный уровень — разработан Netscape для обеспечения секретности и защищенности информации при передаче данных через Интернет. Поддерживает идентификацию сервера и клиента и обеспечивает защищенность и целостность канала передачи. Работает на транспортном уровне и ко-

пирует «библиотеку сокетов», делая ее независимой от приложений. Шифрует весь канал связи, не поддерживает цифровые подписи и не работает на сеансовом уровне.

Symmetric algorithm, conventional, secret key, and single key algorithms. Симметричный или стандартный алгоритм, а также алгоритм секретного или одного ключа — алгоритм, в котором ключ шифрования и расшифровки или одинаковы, либо вычисляются один из другого. Существует два вида: блочный и потоковый.

Subkey. Подключ — ключ Диффи-Хеллмана, который включается в состав главного ключа. Его можно в любой момент аннулировать, без последствий для главного ключа и для подписей, созданных с его помощью.

Text standard, printable, 7-bit ASCII text — стандартный, пригодный для печати 7-битовый ASCII текст.

Timestamping — запись времени создания или времени существования информации.

TLS (Transport Layer Security). Защита транспортного уровня — проект IETF, первая версия базируется на SSL версии 3.0, и предоставляет закрытость соединения через Интернет.

TLSP (Transport Layer Security Protocol). Защитный протокол транспортного уровня — проект межнационального стандарта ISO 10736.

Triple DES. Тройной DES — структура шифрования данных, в которой алгоритм DES используется три раза с тремя различными ключами.

Trusted. Удостоверенный — открытый ключ считается удостоверенным вами, если он был подписан вами или же тем, кого вы признаете посредником.

Trusted introducer. Доверенный посредник — тот, чьему утверждения подлинности ключа вы доверяете. Когда доверенный посредник подписывает чей-то ключ, вы верите, что этот ключ – подлинный, и вам не нужно проверять его перед использованием.

User ID. Имя пользователя — текстовая фраза, идентифицирующая пару ключей. Общепринятым именем пользователя является имя и электронный адрес владельца ключа. Имя пользователя помогает

пользователям (и самому владельцу ключа и его коллегам) идентифицировать владельца пары ключей.

Validity. Достоверность — показывает уровень конфиденциальности, которую имеет ключ конкретного пользователя.

Verification. Проверка — процедура сравнения подписи, созданной с помощью закрытого ключа, с открытым ключом. Проверка подтверждает, что информация была послана подписавшимся лицом, и сообщение на было подменено посторонним.

VPN (Virtual Private Network). Виртуальная частная сеть — позволяет создавать частные сети, связывающие конечных пользователей через общую сеть (Интернет), подобно сетям Интранет в организациях.

Web of trust. Паутина доверия — распределенная модель доверия, используемая PGP для подтверждения принадлежности открытого ключа, где используется кумулятивный уровень доверия, зависимый от личных знаний каждого посредника.

X.509 — цифровой сертификат ITU-T, который являет собой электронный документ, используемый для доказательства тождественности и принадлежности открытого ключа. Он содержит имя лица, выдавшего информацию для идентификации пользователя, цифровую подпись лица, выдавшего сертификат и другие сведения.

Литература

1. An Introduction to Cryptography. http://www.pgpru.com.

2. PGP Desktop Security for Windows 95, Windows 98, and Windows NT. User's Guide. Version 6.5 Int. — Network Associates, Inc., 1999.

3. Яннамико, М. PGP для Персональной приватности, версия 5.0: Пер. с англ. / М. Яннамико. — Pretty Good Privacy, Inc., 1997. http://www.geocities.com/SoHo/Studios/1059/pgp-ru.html.

4. Столлингс, В. Основы защиты сетей. Приложения и стандарты: Пер. с англ. / В. Столлингс. — М.: Вильямс, 2002. — 432 с.

5. Крупник, А. Бизнес в Интернет. / А. Крупник. — М.: МикроАрт, 2002. — 240 с.

6. Информационные технологии в бизнесе. / Под ред. М. Желены. — СПб.: Питер, 2002. — 1120 с.

7. Голдовский, И. Безопасность платежей в Интернете. / И. Голдовский. — СПб: Питер, 2001. — 240 с.

8. Международный отчет о ситуации с криптографией. Electronic Privacy Information Center. First edition 2000. http://www.hro.org.

9. Мясникова, Л.А. Постмодерн коммерции (трансформация коммерции в современном обществе). / Л.А. Мясникова, М.И Фрид. — СПб.: Бизнес-пресса, 2001. — 208 с.

10. Stallings, W. Technical Resources and Course Web Site for Network Security Essentials: Applications and Standards. http://william-stallings.com/NetSec.html.

11. Brassard, J. Modern Criptology. Springer-Verlag, Berlin, 1988. — 107 p. http://cins.ict.nsc.ru/citonod/My/Crypto/Brassard.html.

12. Tatu Ylonen. Introduction to Cryptography. Введение в криптографию. http://www.ssl.stu.neva.ru/psw/crypto/intro.html.

13. PGP. http://pgp2all.org.ru/pgp-for-all.html.

14. PGP в России. http://www.pgpru.com.

15. MIT PGP Public Key Server. http://pgpkeys.mit.edu.

16. Смирнов, С. Словарь терминов. http://www.pgpru.com.

17. Приходько, А.Я. Словарь-справочник по информационной безопасности. / А.Я. Приходько. — М.: СИНТЕГ, 2001. — 124 с.

18. Когаловский, М.Р. Перспективные технологии информационных систем. / М.Р. Когаловский. — М.: АйТи, 2003. — 288 с.

19. Домашняя страница Фила Зиммермана. http://www.philzimmermann.com.

20. Драница А. Хранитель секретов. http://www.computerra.ru/offline/2003/512/29689/.

21. Спецификации IETF-стандарта OpenPGP. RFC 2440: Open PGP Message Format. http://www.ietf.org/rfc/rfc2440.txt.

22. Корпоративный портал PGP Corporation. http://www.pgp.com.

23. The International PGP Home Page. http://www.pgpi.org.

Оглавление